National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
01 – 15 Jun 2023 Vol. 10 No. 11

Table of Content

Vendor	Product	Page Number
Qualcomm	qca9882	912
	qca9886	912
	qca9887	913
	qca9888	913
	qca9889	914
	qca9898	915
	qca9980	916
	qca9982	916
	qca9984	917
	qca9985	917
	qca9986	918
	qca9990	919
	qca9992	920
	qca9994	920
	qcc2073	921
	qcc2076	922
	qcm2290	923
	qcm4290	924
	qcm4325	925
	qcm4490	926
	qcm6125	927
	qcm6490	928
	qcn5021	929
	qcn5022	929
	qcn5024	930
	qcn5052	931
	qcn5054	932
	qcn5064	933
	qcn5121	933
	qcn5122	933
	qcn5124	934
	qcn5152	935

Vendor	Product	Page Number
Qualcomm	sc8180x-ab	984
	sc8180x-ac	985
	sc8180x-ad	985
	sc8180x-af	985
	sc8180xp-aa	986
	sc8180xp-ab	986
	sc8180xp-ac	987
	sc8180xp-ad	987
	sc8180xp-af	987
	sc8180x\+sdx55	988
	sc8280xp-ab	988
	sc8280xp-bb	989
	sd460	989
	sd660	990
	sd662	990
	sd670	991
	sd675	991
	sd730	992
	sd820	993
	sd821	993
	sd835	993
	sd855	994
	sd865_5g	994
	sd888	996
	sda845	997
	sdm429	997
	sdm429w	998
	sdm439	999
	sdm660	1000
	sdm670	1001
	sdm710	1001
	sdm712	1002

Vendor	Product	Page Number
Qualcomm	sm7325	1025
	sm7325-ae	1026
	sm7325-af	1026
	sm7325p	1027
	sm7350-ab	1028
	sm8150	1029
	sm8150-ac	1030
	sm8250	1030
	sm8250-ab	1032
	sm8250-ac	1033
	sm8350	1034
	sm8350-ac	1035
	sm8450	1036
	sm8475	1037
	smart_audio_200_platform	1038
	smart_audio_400_platform	1038
	snapdragonwear_4100\+_platform	1039
	snapdragon_210_processor	1039
	snapdragon_212_mobile_platform	1040
	snapdragon_630_mobile_platform	1040
	snapdragon_636_mobile_platform	1040
	snapdragon_652_mobile_platform	1040
	snapdragon_662_mobile_platform	1041
	snapdragon_675_mobile_platform	1041
	snapdragon_680_4g_mobile_platform	1042
	snapdragon_690_5g_mobile_platform	1042
	snapdragon_695_5g_mobile_platform	1043
	snapdragon_7c\+_gen3_compute	1043
	snapdragon_7c\+_gen_3_compute	1043
	snapdragon_808_processor	1044
	snapdragon_810_processor	1044
	snapdragon_820_automotive_platform	1044

Vendor	Product	Page Number
Qualcomm	snapdragon_820_mobile_platform	1045
	snapdragon_821_mobile_platform	1045
	snapdragon_835_mobile_pc_platform	1045
	snapdragon_845_mobile_platform	1046
	snapdragon_850_mobile_compute_platform	1046
	snapdragon_ar2_gen1_platform	1046
	snapdragon_ar2_gen_1_platform	1047
	snapdragon_auto_4g_modem	1048
	snapdragon_auto_5g_modem-rf	1048
	snapdragon_w5\+_gen1_wearable_platform	1049
	snapdragon_w5\+_gen_1_wearable_platform	1049
	snapdragon_x12_lte_modem	1050
	snapdragon_x20_lte_modem	1050
	snapdragon_x24_lte_modem	1051
	snapdragon_x50_5g_modem-rf_system	1051
	snapdragon_x55_5g_modem-rf_system	1052
	snapdragon_x5_lte_modem	1053
	snapdragon_x65_5g_modem-rf_system	1053
	snapdragon_xr1_platform	1054
	snapdragon_xr2\+_gen1_platform	1055
	snapdragon_xr2\+_gen_1_platform	1055
	snapdragon_xr2_5g_platform	1056
	ssg2115p	1057
	ssg2125p	1058
	sw5100	1059
	sw5100p	1060
	sxr1120	1061
	sxr1230p	1062
	sxr2130	1063
	sxr2230p	1064
	vision_intelligence_300_platform	1065
	vision_intelligence_400_platform	1065

Vendor	Product	Page Number
Draytek	vigor167_firmware	1197
	vigor2135ac_firmware	1198
	vigor2135ax_firmware	1200
	vigor2135fvac_firmware	1201
	vigor2135vac_firmware	1202
	vigor2620ln_firmware	1203
	vigor2620l_firmware	1204
	vigor2763ac_firmware	1206
	vigor2765ac_firmware	1207
	vigor2765ax_firmware	1208
	vigor2765vac_firmware	1209
	vigor2766ac_firmware	1211
	vigor2766ax_firmware	1212
	vigor2766vac_firmware	1213
	vigor2832n_firmware	1214
	vigor2862ac_firmware	1215
	vigor2862bn_firmware	1217
	vigor2862b_firmware	1218
	vigor2862lac_firmware	1219
	vigor2862ln_firmware	1220
	vigor2862l_firmware	1221
	vigor2862n_firmware	1223
	vigor2862vac_firmware	1224
	vigor2865ac_firmware	1225
	vigor2865ax_firmware	1226
	vigor2865lac_firmware	1228
	vigor2865l_firmware	1229
	vigor2865vac_firmware	1230
	vigor2866ac_firmware	1231
	vigor2866ax_firmware	1232
	vigor2866lac_firmware	1234
	vigor2866l_firmware	1235

Vendor	Product	Page Number
Draytek	vigor2866vac_firmware	1236
	vigor2915ac_firmware	1237
	vigor2926_plus_firmware	1238
	vigor2927ac_firmware	1240
	vigor2927ax_firmware	1241
	vigor2927f_firmware	1242
	vigor2927lac_firmware	1243
	vigor2927l_firmware	1245
	vigor2927vac_firmware	1246
	vigor2962_firmware	1247
	vigor3910_firmware	1248
	vigorap_1000c_firmware	1249
	vigorap_1060c_firmware	1250
	vigorap_903_firmware	1251
	vigorap_906_firmware	1251
	vigorap_912c_firmware	1252
	vigorap_918r_firmware	1253
	vigorap_960c_firmware	1253
	vigorlte_200n_firmware	1254
	vigorswitch_fx2120_firmware	1255
	vigorswitch_g1080_firmware	1256
	vigorswitch_g1085_firmware	1256
	vigorswitch_g1282_firmware	1257
	vigorswitch_g2100_firmware	1257
	vigorswitch_g2121_firmware	1258
	vigorswitch_g2280x_firmware	1259
	vigorswitch_g2540xs_firmware	1259
	vigorswitch_p1282_firmware	1260
	vigorswitch_p2100_firmware	1261
	vigorswitch_p2280x_firmware	1261
	vigorswitch_p2540xs_firmware	1262
	vigorswitch_pq2121x_firmware	1262

Vendor	Product	Page Number
Qualcomm	ar9380_firmware	1314
	c-v2x9150_firmware	1315
	csr8811_firmware	1315
	csra6620_firmware	1316
	csra6640_firmware	1317
	csrb31024_firmware	1318
	flight_rb5_5g_platform_firmware	1318
	home_hub_100_platform_firmware	1319
	immersive_home_214_platform_firmware	1319
	immersive_home_216_platform_firmware	1320
	immersive_home_316_platform_firmware	1321
	immersive_home_318_platform_firmware	1322
	ipq4018_firmware	1323
	ipq4019_firmware	1323
	ipq4028_firmware	1324
	ipq4029_firmware	1324
	ipq5010_firmware	1324
	ipq5028_firmware	1325
	ipq6000_firmware	1326
	ipq6005_firmware	1327
	ipq6010_firmware	1327
	ipq6018_firmware	1328
	ipq6028_firmware	1329
	ipq8064_firmware	1330
	ipq8065_firmware	1331
	ipq8068_firmware	1332
	ipq8069_firmware	1332
	ipq8070a_firmware	1333
	ipq8070_firmware	1333
	ipq8071a_firmware	1334
	ipq8071_firmware	1335
	ipq8072a_firmware	1335

Vendor	Product	Page Number
Qualcomm	ipq8072_firmware	1336
	ipq8074a_firmware	1336
	ipq8074_firmware	1337
	ipq8076a_firmware	1337
	ipq8076_firmware	1338
	ipq8078a_firmware	1339
	ipq8078_firmware	1340
	ipq8173_firmware	1341
	ipq8174_firmware	1342
	ipq9008_firmware	1343
	ipq9574_firmware	1344
	mdm8215_firmware	1344
	mdm9215_firmware	1345
	mdm9250_firmware	1345
	mdm9310_firmware	1345
	mdm9615_firmware	1345
	mdm9628_firmware	1346
	mdm9640_firmware	1346
	mdm9645_firmware	1346
	mdm9650_firmware	1346
	msm8996au_firmware	1347
	pmp8074_firmware	1347
	qam8255p_firmware	1347
	qam8295p_firmware	1348
	qam8650p_firmware	1350
	qam8775p_firmware	1350
	qca0000_firmware	1351
	qca1023_firmware	1352
	qca1062_firmware	1352
	qca1064_firmware	1352
	qca1990_firmware	1352
	qca2062_firmware	1353

Vendor	Product	Page Number
Qualcomm	qca2064_firmware	1353
	qca2065_firmware	1354
	qca2066_firmware	1354
	qca4010_firmware	1354
	qca4024_firmware	1355
	qca4531_firmware	1355
	qca6174a_firmware	1356
	qca6174_firmware	1356
	qca6175a_firmware	1357
	qca6310_firmware	1357
	qca6320_firmware	1358
	qca6335_firmware	1358
	qca6390_firmware	1359
	qca6391_firmware	1360
	qca6420_firmware	1362
	qca6421_firmware	1363
	qca6426_firmware	1363
	qca6428_firmware	1364
	qca6430_firmware	1365
	qca6431_firmware	1365
	qca6436_firmware	1366
	qca6438_firmware	1367
	qca6554a_firmware	1367
	qca6564au_firmware	1368
	qca6564a_firmware	1369
	qca6564_firmware	1369
	qca6574au_firmware	1370
	qca6574a_firmware	1371
	qca6574_firmware	1372
	qca6584au_firmware	1373
	qca6584_firmware	1374
	qca6595au_firmware	1374

Vendor	Product	Page Number
Qualcomm	qca6595_firmware	1376
	qca6678aq_firmware	1377
	qca6696_firmware	1378
	qca6698aq_firmware	1379
	qca6797aq_firmware	1380
	qca7500_firmware	1381
	qca8072_firmware	1381
	qca8075_firmware	1382
	qca8081_firmware	1383
	qca8082_firmware	1384
	qca8084_firmware	1385
	qca8085_firmware	1386
	qca8337_firmware	1386
	qca8386_firmware	1387
	qca9367_firmware	1388
	qca9377_firmware	1388
	qca9379_firmware	1389
	qca9531_firmware	1389
	qca9558_firmware	1390
	qca9561_firmware	1390
	qca9880_firmware	1390
	qca9882_firmware	1390
	qca9886_firmware	1390
	qca9887_firmware	1391
	qca9888_firmware	1391
	qca9889_firmware	1392
	qca9898_firmware	1393
	qca9980_firmware	1394
	qca9982_firmware	1394
	qca9984_firmware	1395
	qca9985_firmware	1395
	qca9986_firmware	1396

Vendor	Product	Page Number
Qualcomm	qca9990_firmware	1397
	qca9992_firmware	1398
	qca9994_firmware	1398
	qcc2073_firmware	1399
	qcc2076_firmware	1400
	qcm2290_firmware	1401
	qcm4290_firmware	1402
	qcm4325_firmware	1403
	qcm4490_firmware	1404
	qcm6125_firmware	1405
	qcm6490_firmware	1406
	qcn5021_firmware	1407
	qcn5022_firmware	1407
	qcn5024_firmware	1408
	qcn5052_firmware	1409
	qcn5054_firmware	1410
	qcn5064_firmware	1411
	qcn5121_firmware	1411
	qcn5122_firmware	1411
	qcn5124_firmware	1412
	qcn5152_firmware	1413
	qcn5154_firmware	1414
	qcn5164_firmware	1415
	qcn5550_firmware	1416
	qcn6023_firmware	1416
	qcn6024_firmware	1417
	qcn6100_firmware	1418
	qcn6102_firmware	1419
	qcn6112_firmware	1419
	qcn6122_firmware	1420
	qcn6132_firmware	1421
	qcn7605_firmware	1422

Vendor	Product	Page Number
Qualcomm	qcn7606_firmware	1422
	qcn9000_firmware	1422
	qcn9001_firmware	1423
	qcn9002_firmware	1424
	qcn9003_firmware	1425
	qcn9011_firmware	1425
	qcn9012_firmware	1426
	qcn9022_firmware	1426
	qcn9024_firmware	1427
	qcn9070_firmware	1429
	qcn9072_firmware	1430
	qcn9074_firmware	1431
	qcn9100_firmware	1432
	qcn9274_firmware	1433
	qcs2290_firmware	1434
	qcs400_firmware	1435
	qcs410_firmware	1435
	qcs4290_firmware	1436
	qcs4490_firmware	1437
	qcs605_firmware	1438
	qcs610_firmware	1438
	qcs6125_firmware	1439
	qcs6490_firmware	1440
	qcs8155_firmware	1441
	qcs8250_firmware	1441
	qcs8550_firmware	1442
	qfe1922_firmware	1443
	qfe1952_firmware	1443
	qm215_firmware	1443
	qrb5165m_firmware	1444
	qrb5165n_firmware	1445
	qrb5165_firmware	1445

Vendor	Product	Page Number
Qualcomm	qsm8250_firmware	1446
	qsm8350_firmware	1446
	robotics_rb3_platform_firmware	1447
	sa4150p_firmware	1447
	sa4155p_firmware	1448
	sa6145p_firmware	1449
	sa6150p_firmware	1450
	sa6155p_firmware	1451
	sa6155_firmware	1452
	sa8145p_firmware	1453
	sa8150p_firmware	1454
	sa8155p_firmware	1455
	sa8155_firmware	1456
	sa8195p_firmware	1457
	sa8255p_firmware	1458
	sa8295p_firmware	1459
	sa8540p_firmware	1460
	sa9000p_firmware	1461
	sc7180-ac_firmware	1461
	sc7180-ad_firmware	1461
	sc8180x-aa_firmware	1462
	sc8180x-ab_firmware	1462
	sc8180x-ac_firmware	1463
	sc8180x-ad_firmware	1463
	sc8180x-af_firmware	1463
	sc8180xp-aa_firmware	1464
	sc8180xp-ab_firmware	1464
	sc8180xp-ac_firmware	1465
	sc8180xp-ad_firmware	1465
	sc8180xp-af_firmware	1465
	sc8180x\+sdx55_firmware	1466
	sc8280xp-ab_firmware	1466

Vendor	Product	Page Number
Qualcomm	sc8280xp-bb_firmware	1467
	sd460_firmware	1467
	sd660_firmware	1468
	sd662_firmware	1468
	sd670_firmware	1469
	sd675_firmware	1469
	sd730_firmware	1470
	sd820_firmware	1471
	sd821_firmware	1471
	sd835_firmware	1471
	sd855_firmware	1472
	sd865_5g_firmware	1472
	sd888_firmware	1474
	sda845_firmware	1475
	sdm429w_firmware	1475
	sdm429_firmware	1476
	sdm439_firmware	1477
	sdm660_firmware	1478
	sdm670_firmware	1479
	sdm710_firmware	1479
	sdm712_firmware	1480
	sdm845_firmware	1480
	sdx20m_firmware	1480
	sdx55_firmware	1481
	sd_455_firmware	1482
	sd_675_firmware	1482
	sd_8cx_firmware	1482
	sd_8_gen1_5g_firmware	1483
	sg4150p_firmware	1483
	sm4125_firmware	1484
	sm4250-aa_firmware	1485
	sm4350-ac_firmware	1486

Vendor	Product	Page Number
Qualcomm	sm4350_firmware	1487
	sm4375_firmware	1487
	sm4450_firmware	1488
	sm6125_firmware	1489
	sm6150-ac_firmware	1490
	sm6225-ad_firmware	1491
	sm6225_firmware	1491
	sm6250p_firmware	1492
	sm6250_firmware	1493
	sm6350_firmware	1494
	sm6375_firmware	1494
	sm7125_firmware	1495
	sm7150-aa_firmware	1496
	sm7150-ab_firmware	1497
	sm7150-ac_firmware	1497
	sm7225_firmware	1498
	sm7250-aa_firmware	1499
	sm7250-ab_firmware	1500
	sm7250-ac_firmware	1501
	sm7250p_firmware	1501
	sm7315_firmware	1502
	sm7325-ae_firmware	1503
	sm7325-af_firmware	1504
	sm7325p_firmware	1504
	sm7325_firmware	1505
	sm7350-ab_firmware	1506
	sm8150-ac_firmware	1507
	sm8150_firmware	1508
	sm8250-ab_firmware	1508
	sm8250-ac_firmware	1510
	sm8250_firmware	1511
	sm8350-ac_firmware	1512

Vendor	Product	Page Number
Qualcomm	sm8350_firmware	1513
	sm8450_firmware	1514
	sm8475_firmware	1515
	smart_audio_200_platform_firmware	1516
	smart_audio_400_platform_firmware	1516
	snapdragonwear_4100\+_platform_firmware	1517
	snapdragon_210_processor_firmware	1517
	snapdragon_212_mobile_platform_firmware	1518
	snapdragon_630_mobile_platform_firmware	1518
	snapdragon_636_mobile_platform_firmware	1518
	snapdragon_652_mobile_platform_firmware	1518
	snapdragon_662_mobile_platform_firmware	1519
	snapdragon_675_mobile_platform_firmware	1519
	snapdragon_680_4g_mobile_platform_firmware	1520
	snapdragon_690_5g_mobile_platform_firmware	1520
	snapdragon_695_5g_mobile_platform_firmware	1521
	snapdragon_7c\+_gen3_compute_firmware	1521
	snapdragon_7c\+_gen_3_compute_firmware	1521
	snapdragon_808_processor_firmware	1522
	snapdragon_810_processor_firmware	1522
	snapdragon_820_automotive_platform_firmware	1522
	snapdragon_820_mobile_platform_firmware	1523
	snapdragon_821_mobile_platform_firmware	1523
	snapdragon_835_mobile_pc_platform_firmware	1523
	snapdragon_845_mobile_platform_firmware	1524
	snapdragon_850_mobile_compute_platform_firmware	1524
	snapdragon_ar2_gen1_platform_firmware	1524
	snapdragon_ar2_gen_1_platform_firmware	1525

Vendor	Product	Page Number
Qualcomm	snapdragon_auto_4g_modem_firmware	1526
	snapdragon_auto_5g_modem-rf_firmware	1526
	snapdragon_w5\+_gen1_wearable_platform_firmware	1527
	snapdragon_w5\+_gen_1_wearable_platform_firmware	1527
	snapdragon_x12_lte_modem_firmware	1528
	snapdragon_x20_lte_modem_firmware	1528
	snapdragon_x24_lte_modem_firmware	1529
	snapdragon_x50_5g_modem-rf_system_firmware	1529
	snapdragon_x55_5g_modem-rf_system_firmware	1530
	snapdragon_x5_lte_modem_firmware	1531
	snapdragon_x65_5g_modem-rf_system_firmware	1531
	snapdragon_xr1_platform_firmware	1532
	snapdragon_xr2\+_gen1_platform_firmware	1533
	snapdragon_xr2\+_gen_1_platform_firmware	1533
	snapdragon_xr2_5g_platform_firmware	1534
	ssg2115p_firmware	1535
	ssg2125p_firmware	1536
	sw5100p_firmware	1537
	sw5100_firmware	1538
	sxr1120_firmware	1539
	sxr1230p_firmware	1540
	sxr2130_firmware	1541
	sxr2230p_firmware	1542
	vision_intelligence_300_platform_firmware	1543
	vision_intelligence_400_platform_firmware	1543
	wcd9326_firmware	1544
	wcd9330_firmware	1545
	wcd9335_firmware	1545
	wcd9340_firmware	1546

Vendor	Product	Page Number
Qualcomm	wcd9341_firmware	1547
	wcd9360_firmware	1548
	wcd9370_firmware	1548
	wcd9371_firmware	1550
	wcd9375_firmware	1551
	wcd9380_firmware	1552
	wcd9385_firmware	1554
	wcn3610_firmware	1555
	wcn3615_firmware	1556
	wcn3620_firmware	1556
	wcn3660b_firmware	1558
	wcn3680b_firmware	1559
	wcn3680_firmware	1560
	wcn3910_firmware	1560
	wcn3950_firmware	1561
	wcn3980_firmware	1563
	wcn3988_firmware	1564
	wcn3990_firmware	1565
	wcn3991_firmware	1566
	wcn3998_firmware	1567
	wcn3999_firmware	1568
	wcn6740_firmware	1569
	wcn6750_firmware	1570
	wcn685x-1_firmware	1571
	wcn685x-5_firmware	1573
	wcn785x-1_firmware	1575
	wcn785x-5_firmware	1576
	wsa8810_firmware	1577
	wsa8815_firmware	1579
	wsa8830_firmware	1580
	wsa8832_firmware	1582
	wsa8835_firmware	1583

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 07fly					
Product: customer_relationship_management					
Affected Version(s): * Up to (including) 1.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-2023	5.4	A vulnerability was found in 07FLY CRM up to 1.2.0. It has been declared as problematic. This vulnerability affects unknown code of the component User Profile Handler. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-230560. **CVE ID : CVE-2023-3058**	N/A	A-07F-CUST-280623/1
Vendor: 10web					
Product: 10web_social_post_feed					
Affected Version(s): * Up to (excluding) 1.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2023	6.1	The 10Web Social Post Feed WordPress plugin before 1.2.9 does not sanitise and escape some parameter before outputting it back in a page, leading to a Reflected Cross-Site Scripting which could	N/A	A-10W-10WE-280623/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used against high privilege users such as admin **CVE ID : CVE-2023-2503**		
Product: seo					
Affected Version(s): * Up to (excluding) 1.2.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2023	4.8	The SEO by 10Web WordPress plugin before 1.2.7 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-2023-2224**	N/A	A-10W-SEO-280623/3
Vendor: Admidio					
Product: admidio					
Affected Version(s): * Up to (excluding) 4.2.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository admidio/admidio prior to 4.2.8. **CVE ID : CVE-2023-3109**	https://huntr.dev/bounties/6fa6070e-8f7f-43ae-8a84-e36b28256123, https://github.com/admidio/admidio/commit/a7c211b835cafe1158	A-ADM-ADMI-280623/4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				932fbfcff9e5552e57510a	
Vendor: advanced-woo-search					
Product: advanced_woo_search					
Affected Version(s): * Up to (including) 2.77					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	4.4	The Advanced Woo Search plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 2.77 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-2452**	https://plugins.trac.wordpress.org/browser/advanced-woo-search/tags/2.77/includes/admin/class-aws-admin-options.php#L473, https://plugins.trac.wordpress.org/browser/advanced-woo-search/tags/2.77/includes/admin/class-aws-admin-options.php#L481	A-ADV-ADVA-280623/5
Vendor: Advantech					
Product: webaccess					
Affected Version(s): 8.4.5					
Insufficient Verification of Data	07-Jun-2023	7.8	If an attacker can trick an authenticated user into loading a	N/A	A-ADV-WEBA-280623/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			maliciously crafted .zip file onto Advantech WebAccess version 8.4.5, a web shell could be used to give the attacker full control of the SCADA server. **CVE ID : CVE-2023-2866**		
Product: webaccess\/scada					
Affected Version(s): * Up to (including) 9.1.3					
Improper Control of Generation of Code ('Code Injection')	06-Jun-2023	9.8	In Advantech WebAccss/SCADA v9.1.3 and prior, there is an arbitrary file overwrite vulnerability, which could allow an attacker to overwrite any file in the operating system (including system files), inject code into an XLS file, and modify the file extension, which could lead to arbitrary code execution. **CVE ID : CVE-2023-32540**	N/A	A-ADV-WEBA-280623/7
Unrestricted Upload of File with	06-Jun-2023	9.8		N/A	A-ADV-WEBA-280623/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			In Advantech WebAccss/SCADA v9.1.3 and prior, there is an arbitrary file upload vulnerability that could allow an attacker to modify the file extension of a certificate file to ASP when uploading it, which can lead to remote code execution. **CVE ID : CVE-2023-32628**		
Unrestricted Upload of File with Dangerous Type	06-Jun-2023	7.2	In Advantech WebAccss/SCADA v9.1.3 and prior, there is an arbitrary file upload vulnerability that could allow an attacker to upload an ASP script file to a webserver when logged in as manager user, which can lead to arbitrary code execution.	N/A	A-ADV-WEBA-280623/9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22450		
Vendor: advent					
Product: tamale_rms					
Affected Version(s): * Up to (excluding) 23.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jun-2023	5.3	Advent/SSC Inc. Tamale RMS < 23.1 is vulnerable to Directory Traversal. If one traverses to the affected URL, one enumerates Contact information on the host which contains usernames, e-mail addresses, and other internal information stored within the web app. **CVE ID : CVE-2023-33524**	N/A	A-ADV-TAMA-280623/10
Vendor: agro-school_management_system_project					
Product: agro-school_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	02-Jun-2023	9.8	A vulnerability was found in code-projects Agro-School Management System 1.0 and classified as critical. This issue affects some unknown processing of the file btn_functions.php of the component Attachment Image Handler. The	N/A	A-AGR-AGRO-280623/11

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation leads to unrestricted upload. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-230567. **CVE ID : CVE-2023-3061**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	A vulnerability was found in code-projects Agro-School Management System 1.0. It has been classified as critical. Affected is an unknown function of the file index.php. The manipulation of the argument password leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-230568. **CVE ID : CVE-2023-3062**	N/A	A-AGR-AGRO-280623/12
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jun-2023	9.8	A vulnerability classified as critical has been found in code-projects Agro-School Management System 1.0. Affected is the function doUpdateQuestion of the file btn_functions.php. The manipulation of the argument question_id leads to sql injection. It is possible to launch	N/A	A-AGR-AGRO-280623/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attack remotely. The exploit has been disclosed to the public and may be used. VDB-230670 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3094**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-2023	5.4	A vulnerability has been found in code-projects Agro-School Management System 1.0 and classified as problematic. This vulnerability affects the function doAddQuestion of the file btn_functions.php. The manipulation of the argument Question leads to cross site scripting. The attack can be initiated remotely. VDB-230566 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3060**	N/A	A-AGR-AGRO-280623/14
Vendor: alist_project					
Product: alist					
Affected Version(s): * Up to (excluding) 3.16.3					
Unrestricted Upload of File with Dangerous Type	07-Jun-2023	8.8	alist <=3.16.3 is vulnerable to Incorrect Access Control. Low privilege accounts can upload any file. **CVE ID : CVE-2023-33498**	N/A	A-ALI-ALIS-280623/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Apache					
Product: guacamole					
Affected Version(s): * Up to (excluding) 1.5.2					
Incorrect Calculation of Buffer Size	07-Jun-2023	7.5	Apache Guacamole 1.5.1 and older may incorrectly calculate the lengths of instruction elements sent during the Guacamole protocol handshake, potentially allowing an attacker to inject Guacamole instructions during the handshake through specially-crafted data. **CVE ID : CVE-2023-30575**	N/A	A-APA-GUAC-280623/16
Affected Version(s): From (including) 0.9.0 Up to (excluding) 1.5.2					
Use After Free	07-Jun-2023	8.1	Apache Guacamole 0.9.10 through 1.5.1 may continue to reference a freed RDP audio input buffer. Depending on timing, this may allow an attacker to execute arbitrary code with the privileges of the guacd process. **CVE ID : CVE-2023-30576**	https://lists.apache.org/thread/vgtvxb3w7mm84hx6v8dfc0onsoz05gb6	A-APA-GUAC-280623/17
Vendor: ARM					
Product: avalon_gpu_kernel_driver					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) r41p0 Up to (excluding) r43p0					
N/A	02-Jun-2023	5.5	An issue was discovered in the Arm Mali GPU Kernel Driver. A non-privileged user can make improper GPU processing operations to gain access to already freed memory. This affects Midgard r29p0 through r32p0, Bifrost r17p0 through r42p0 before r43p0, Valhall r19p0 through r42p0 before r43p0, and Arm's GPU Architecture Gen5 r41p0 through r42p0 before r43p0. **CVE ID : CVE-2023-28147**	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities	A-ARM-AVAL-280623/18
N/A	02-Jun-2023	5.5	An issue was discovered in the Arm Mali GPU Kernel Driver. A non-privileged user can make improper GPU processing operations to gain access to already freed memory. This affects Valhall r29p0 through r42p0 before r43p0, and Arm's GPU Architecture Gen5 r41p0 through r42p0 before r43p0. **CVE ID : CVE-2023-28469**	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities	A-ARM-AVAL-280623/19
Product: bifrost_gpu_kernel_driver					
Affected Version(s): From (including) r17p0 Up to (excluding) r43p0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jun-2023	5.5	An issue was discovered in the Arm Mali GPU Kernel Driver. A non-privileged user can make improper GPU processing operations to gain access to already freed memory. This affects Midgard r29p0 through r32p0, Bifrost r17p0 through r42p0 before r43p0, Valhall r19p0 through r42p0 before r43p0, and Arm's GPU Architecture Gen5 r41p0 through r42p0 before r43p0. **CVE ID : CVE-2023-28147**	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities	A-ARM-BIFR-280623/20
Product: midgard_gpu_kernel_driver					
Affected Version(s): From (including) r29p0 Up to (including) r32p0					
N/A	02-Jun-2023	5.5	An issue was discovered in the Arm Mali GPU Kernel Driver. A non-privileged user can make improper GPU processing operations to gain access to already freed memory. This affects Midgard r29p0 through r32p0, Bifrost r17p0 through r42p0 before r43p0, Valhall r19p0 through r42p0 before r43p0, and Arm's GPU Architecture Gen5 r41p0 through r42p0 before r43p0.	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities	A-ARM-MIDG-280623/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28147		
Product: valhall_gpu_kernel_driver					
Affected Version(s): From (including) r19p0 Up to (excluding) r43p0					
N/A	02-Jun-2023	5.5	An issue was discovered in the Arm Mali GPU Kernel Driver. A non-privileged user can make improper GPU processing operations to gain access to already freed memory. This affects Midgard r29p0 through r32p0, Bifrost r17p0 through r42p0 before r43p0, Valhall r19p0 through r42p0 before r43p0, and Arm's GPU Architecture Gen5 r41p0 through r42p0 before r43p0. **CVE ID : CVE-2023-28147**	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities	A-ARM-VALH-280623/22
Affected Version(s): From (including) r29p0 Up to (excluding) r43p0					
N/A	02-Jun-2023	5.5	An issue was discovered in the Arm Mali GPU Kernel Driver. A non-privileged user can make improper GPU processing operations to gain access to already freed memory. This affects Valhall r29p0 through r42p0 before r43p0, and Arm's GPU Architecture Gen5 r41p0 through r42p0 before r43p0.	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities	A-ARM-VALH-280623/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28469		
Vendor: aviplugins					
Product: wp_register_profile_with_shortcode					
Affected Version(s): * Up to (including) 3.5.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jun-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Aviplugins.Com WP Register Profile With Shortcode plugin <= 3.5.7 versions. **CVE ID : CVE-2023-23818**	N/A	A-AVI-WP_R-280623/24
Vendor: avohq					
Product: avo					
Affected Version(s): * Up to (including) 2.33.2					
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	05-Jun-2023	8.8	Avo is an open source ruby on rails admin panel creation framework. The polymorphic field type stores the classes to operate on when updating a record with user input, and does not validate them in the back end. This can lead to unexpected behavior, remote code execution, or application crashes when viewing a manipulated record. This issue has been addressed in commit `ec117882d` which is expected to be included in subsequent releases.	https://github.com/avo-hq/avo/commit/ec117882ddb1b519481bdd046dc3cfa4474e6e17, https://github.com/avo-hq/avo/security/advisories/GHSA-86h2-2g4g-29qx	A-AVO-AVO-280623/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Users are advised to limit access to untrusted users until a new release is made. **CVE ID : CVE-2023-34102**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2023	5.4	Avo is an open source ruby on rails admin panel creation framework. In affected versions some avo fields are vulnerable to Cross Site Scripting (XSS) when rendering html based content. Attackers do need form edit privilege in order to successfully exploit this vulnerability, but the results are stored and no specific timing is required. This issue has been addressed in commit `7891c01e` which is expected to be included in the next release of avo. Users are advised to configure CSP headers for their application and to limit untrusted user access as a mitigation. **CVE ID : CVE-2023-34103**	https://github.com/avo-hq/avo/commit/7891c01e1fba9ca5d7dbccc43d27f385e5d08563, https://github.com/avo-hq/avo/security/advisories/GHSA-5cr9-5jx3-2g39	A-AVO-AVO-280623/26
Affected Version(s): 3.0.0					
Use of Externally-Controlled Input to Select	05-Jun-2023	8.8	Avo is an open source ruby on rails admin panel creation framework. The polymorphic field type	https://github.com/avo-hq/avo/commit/ec117882ddb1b51948	A-AVO-AVO-280623/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Classes or Code ('Unsafe Reflection')			stores the classes to operate on when updating a record with user input, and does not validate them in the back end. This can lead to unexpected behavior, remote code execution, or application crashes when viewing a manipulated record. This issue has been addressed in commit `ec117882d` which is expected to be included in subsequent releases. Users are advised to limit access to untrusted users until a new release is made. **CVE ID : CVE-2023-34102**	1bdd046dc3cfa4474e6e17, https://github.com/avo-hq/avo/security/advisories/GHSA-86h2-2g4g-29qx	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2023	5.4	Avo is an open source ruby on rails admin panel creation framework. In affected versions some avo fields are vulnerable to Cross Site Scripting (XSS) when rendering html based content. Attackers do need form edit privilege in order to successfully exploit this vulnerability, but the results are stored and no specific timing is required. This issue has been addressed in	https://github.com/avo-hq/avo/commit/7891c01e1fba9ca5d7dbccc43d27f385e5d08563, https://github.com/avo-hq/avo/security/advisories/GHSA-5cr9-5jx3-2g39	A-AVO-AVO-280623/28

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commit `7891c01e` which is expected to be included in the next release of avo. Users are advised to configure CSP headers for their application and to limit untrusted user access as a mitigation. **CVE ID : CVE-2023-34103**		
Vendor: axtls_project					
Product: axtls					
Affected Version(s): 2.1.5					
Out-of-bounds Write	06-Jun-2023	5.5	axTLS v2.1.5 was discovered to contain a heap buffer overflow in the bi_import function in axtls-code/crypto/bigint.c. This vulnerability allows attackers to cause a Denial of Service (DoS) when parsing a private key. **CVE ID : CVE-2023-33613**	N/A	A-AXT-AXTL-280623/29
Vendor: ays-pro					
Product: quiz_maker					
Affected Version(s): * Up to (excluding) 6.4.2.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2023	6.1	The Quiz Maker WordPress plugin before 6.4.2.7 does not escape some parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting which could be used against high	N/A	A-AYS-QUIZ-280623/30

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege users such as admin **CVE ID : CVE-2023-2571**		
Product: survey_maker					
Affected Version(s): * Up to (excluding) 3.4.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2023	6.1	The Survey Maker WordPress plugin before 3.4.7 does not escape some parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-2572**	N/A	A-AYS-SURV-280623/31
Vendor: azexo					
Product: page_builder_with_image_map_by_azexo					
Affected Version(s): * Up to (including) 1.27.133					
Cross-Site Request Forgery (CSRF)	03-Jun-2023	8.8	The Page Builder by AZEXO plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.27.133. This is due to missing or incorrect nonce validation on the 'azh_add_post', 'azh_duplicate_post', 'azh_update_post' and 'azh_remove_post' functions. This makes it possible for unauthenticated attackers to create,	https://plugins.trac.wordpress.org/browser/page-builder-by-azexo/trunk/azexo_html.php#L4137, https://plugins.trac.wordpress.org/browser/page-builder-by-azexo/trunk/azexo_html.php#L4159	A-AZE-PAGE-280623/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modify, and delete a post via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-3052**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-2023	5.4	The Page Builder by AZEXO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'azh_post' shortcode in versions up to, and including, 1.27.133 due to insufficient input sanitization and output escaping. This makes it possible for contributor-level attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-3051**	https://plugins.trac.wordpress.org/browser/page-builder-by-azexo/trunk/azexo_html.php#L2856, https://plugins.trac.wordpress.org/browser/page-builder-by-azexo/trunk/azexo_html.php#L2845	A-AZE-PAGE-280623/33
Missing Authorization	03-Jun-2023	4.3	The Page Builder by AZEXO plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'azh_add_post' function in versions up to, and including,	https://plugins.trac.wordpress.org/browser/page-builder-by-azexo/trunk/azexo_html.php#L4137, https://plugins.trac.wordpress.org/brows	A-AZE-PAGE-280623/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.27.133. This makes it possible for authenticated attackers to create a post with any post type and post status. **CVE ID : CVE-2023-3053**	er/page-builder-by-azexo/trunk/azexo_html.php#L4085	
Cross-Site Request Forgery (CSRF)	03-Jun-2023	4.3	The Page Builder by AZEXO plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.27.133. This is due to missing or incorrect nonce validation on the 'azh_save' function. This makes it possible for unauthenticated attackers to update the post content and inject malicious JavaScript via a forged request, granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-3055**	https://plugins.trac.wordpress.org/browser/page-builder-by-azexo/trunk/azexo_html.php#L2721	A-AZE-PAGE-280623/35
Vendor: besder					
Product: videoplaytool					
Affected Version(s): 2.0.1.0					
N/A	08-Jun-2023	9.8	Incorrect access control in the administrative functionalities of BES--6024PB-I50H1 VideoPlayTool	N/A	A-BES-VIDE-280623/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v2.0.1.0 allow attackers to execute arbitrary administrative commands via a crafted payload sent to the desired endpoints. **CVE ID : CVE-2023-33443**		
Vendor: Blubrry					
Product: powerpress					
Affected Version(s): * Up to (including) 10.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	5.4	The PowerPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in versions up to, and including, 10.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. NOTE: A partial fix for the issue was introduced in version 10.0.1, and an additional patch (version 10.0.2) was	https://plugins.trac.wordpress.org/changeset/2896729/powerpress, https://plugins.trac.wordpress.org/browser/powerpress/trunk/powerpress-player.php#L102, https://plugins.trac.wordpress.org/changeset/2899207/powerpress	A-BLU-POWE-280623/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			released to address a workaround. **CVE ID : CVE-2023-1917**		
Vendor: booking-wp-plugin					
Product: bookly					
Affected Version(s): * Up to (including) 21.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-2023	4.8	The Bookly plugin for WordPress is vulnerable to Stored Cross-Site Scripting via service titles in versions up to, and including, 21.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with administrative privileges to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-1159**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2913570%40bookly-responsive-appointment-booking-tool&new=2913570%40bookly-responsive-appointment-booking-tool&sfp_email=&sfph_mail=	A-BOO-BOOK-280623/38
Vendor: brizy					
Product: brizy					
Affected Version(s): * Up to (including) 2.4.18					
Insufficient Verification of Data	09-Jun-2023	5.3	The Brizy Page Builder plugin for WordPress is vulnerable to IP	https://plugins.trac.wordpress.org/chang	A-BRI-BRIZ-280623/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			Address Spoofing in versions up to, and including, 2.4.18. This is due to an implicit trust of user-supplied IP addresses in an 'X-Forwarded-For' HTTP header for the purpose of validating allowed IP addresses against a Maintenance Mode whitelist. Supplying a whitelisted IP address within the 'X-Forwarded-For' header allows maintenance mode to be bypassed and may result in the disclosure of potentially sensitive information or allow access to restricted functionality. **CVE ID : CVE-2023-2897**	eset/2919443/brizy	
Vendor: Broadcom					
Product: advanced_secure_gateway					
Affected Version(s): * Up to (excluding) 7.3.13.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Jun-2023	9.8	Advanced Secure Gateway and Content Analysis, prior to 7.3.13.1 / 3.1.6.0, may be susceptible to a Command Injection vulnerability. **CVE ID : CVE-2023-23952**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/22217	A-BRO-ADVA-280623/40
Server-Side	01-Jun-2023	8.1	Advanced Secure Gateway and Content	https://support.broadcom.c	A-BRO-ADVA-280623/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (SSRF)			Analysis, prior to 7.3.13.1 / 3.1.6.0, may be susceptible to a Server-Side Request Forgery vulnerability. **CVE ID : CVE-2023-23955**	om/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/22217	
N/A	01-Jun-2023	7.8	Advanced Secure Gateway and Content Analysis, prior to 7.3.13.1 / 3.1.6.0, may be susceptible to an Elevation of Privilege vulnerability. **CVE ID : CVE-2023-23953**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/22217	A-BRO-ADVA-280623/42
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-2023	5.4	Advanced Secure Gateway and Content Analysis, prior to 7.3.13.1 / 3.1.6.0, may be susceptible to a Stored Cross-Site Scripting vulnerability. **CVE ID : CVE-2023-23954**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/22217	A-BRO-ADVA-280623/43
Product: content_analysis					
Affected Version(s): * Up to (excluding) 3.1.6.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Jun-2023	9.8	Advanced Secure Gateway and Content Analysis, prior to 7.3.13.1 / 3.1.6.0, may be susceptible to a Command Injection vulnerability. **CVE ID : CVE-2023-23952**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/22217	A-BRO-CONT-280623/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	01-Jun-2023	8.1	Advanced Secure Gateway and Content Analysis, prior to 7.3.13.1 / 3.1.6.0, may be susceptible to a Server-Side Request Forgery vulnerability. **CVE ID : CVE-2023-23955**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/22217	A-BRO-CONT-280623/45
N/A	01-Jun-2023	7.8	Advanced Secure Gateway and Content Analysis, prior to 7.3.13.1 / 3.1.6.0, may be susceptible to an Elevation of Privilege vulnerability. **CVE ID : CVE-2023-23953**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/22217	A-BRO-CONT-280623/46
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-2023	5.4	Advanced Secure Gateway and Content Analysis, prior to 7.3.13.1 / 3.1.6.0, may be susceptible to a Stored Cross-Site Scripting vulnerability. **CVE ID : CVE-2023-23954**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/22217	A-BRO-CONT-280623/47
Vendor: bt21_x_bts_wallpaper_project					
Product: bt21_x_bts_wallpaper					
Affected Version(s): 12					
N/A	02-Jun-2023	7.8	The BT21 x BTS Wallpaper app 12 for Android allows unauthorized apps to actively request permission to modify data in the database that records information about a	N/A	A-BT2-BT21-280623/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user's personal preferences and will be loaded into memory to be read and used when the app is opened. An attacker could tamper with this data to cause an escalation of privilege attack. **CVE ID : CVE-2023-29724**		
N/A	02-Jun-2023	5.5	The BT21 x BTS Wallpaper app 12 for Android allows unauthorized applications to actively request permission to insert data into the database that records information about a user's personal preferences and will be loaded into memory to be read and used when the application is opened. By injecting data, the attacker can force the application to load malicious image URLs and display them in the UI. As the amount of data increases, it will eventually cause the application to trigger an OOM error and crash, resulting in a persistent denial of service attack. **CVE ID : CVE-2023-29725**	N/A	A-BT2-BT21-280623/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: bulletin					
Product: announcement_\&_notification_banner_-_bulletin					
Affected Version(s): * Up to (including) 3.6.0					
Missing Authorization	09-Jun-2023	4.3	The Announcement & Notification Banner – Bulletin plugin for WordPress is vulnerable to unauthorized access and modification of data due to a missing capability check on the 'bulletinwp_update_bulletin_status', 'bulletinwp_update_bulletin', 'bulletinwp_update_settings', 'bulletinwp_update_status', 'bulletinwp_export_bulletins', and 'bulletinwp_import_bulletins' functions functions in versions up to, and including, 3.6.0. This makes it possible for authenticated attackers with subscriber-level access, and above, to modify the plugin's settings, modify bulletins, create new bulletins, and more. **CVE ID : CVE-2023-2066**	https://plugins.trac.wordpress.org/changeset/2906036/bulletin-announcements/trunk/classes/class-bulletinwp-ajax.php, https://plugins.trac.wordpress.org/browser/bulletin-announcements/trunk/classes/class-bulletinwp-ajax.php	A-BUL-ANNO-280623/50
Affected Version(s): * Up to (including) 3.7.0					
Cross-Site Request	09-Jun-2023	5.4	The Announcement & Notification Banner –	https://plugins.trac.wordpr	A-BUL-ANNO-280623/51

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Bulletin plugin for WordPress is vulnerable to Cross-Site Request Forgery due to a missing nonce validation on the 'bulletinwp_update_bulletin_status', 'bulletinwp_update_bulletin', 'bulletinwp_update_settings', 'bulletinwp_update_status', 'bulletinwp_export_bulletins', and 'bulletinwp_import_bulletins' functions in versions up to, and including, 3.7.0. This makes it possible for unauthenticated attackers to modify the plugin's settings, modify bulletins, create new bulletins, and more, via a forged request granted they can trick a site's user into performing an action such as clicking on a link. **CVE ID : CVE-2023-2067**	ess.org/changeset/2910991/bulletin-announcements/trunk/classes/class-bulletinwp-ajax.php, https://plugins.trac.wordpress.org/browser/bulletin-announcements/trunk/classes/class-bulletinwp-ajax.php	
Vendor: bytedeco					
Product: javacpp_presets					
Affected Version(s): * Up to (excluding) 1.5.9					
Improper Control of Generation of Code	09-Jun-2023	8.8	JavaCPP Presets is a project providing Java distributions of native C++ libraries. All the actions in the	https://github.com/bytedeco/javacpp-presets/security/advisories	A-BYT-JAVA-280623/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			`bytedeco/javacpp-presets` use the `github.event.head_commit.message?` parameter in an insecure way. For example, the commit message is used in a run statement - resulting in a command injection vulnerability due to string interpolation. No exploitation has been reported. This issue has been addressed in version 1.5.9. Users of JavaCPP Presets are advised to upgrade as a precaution. **CVE ID : CVE-2023-34112**	/GHSA-36rx-hq22-jm5x	
Vendor: Canonical					
Product: landscape					
Affected Version(s): * Up to (excluding) 19.10.5					
Exposure of Resource to Wrong Sphere	06-Jun-2023	8.2	Landscape's server-status page exposed sensitive system information. This data leak included GET requests which contain information to attack and leak further information from the Landscape API. **CVE ID : CVE-2023-32550**	https://bugs.launchpad.net/landscape/+bug/1929037	A-CAN-LAND-280623/53
URL Redirection to Untrusted	06-Jun-2023	6.1	Landscape allowed URLs which caused open redirection.	https://bugs.launchpad.net	A-CAN-LAND-280623/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			**CVE ID : CVE-2023-32551**	/landscape/+bug/1929620	
Vendor: captura_project					
Product: captura					
Affected Version(s): * Up to (including) 8.0.0					
Uncontrolled Search Path Element	04-Jun-2023	7.8	** UNSUPPPORTED WHEN ASSIGNED ** ** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in Captura up to 8.0.0. It has been declared as critical. This vulnerability affects unknown code in the library CRYPTBASE.dll. The manipulation leads to uncontrolled search path. Attacking locally is a requirement. The complexity of an attack is rather high. The exploitation appears to be difficult. The identifier of this vulnerability is VDB-230668. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2023-3091**	N/A	A-CAP-CAPT-280623/55
Vendor: Chamilo					
Product: chamilo_lms					
Affected Version(s): From (including) 1.11.0 Up to (including) 1.11.18					
N/A	08-Jun-2023	8.1	Incorrect access control in Chamilo v1.11.x up to v1.11.18	https://github.com/chamilo/chamilo-	A-CHA-CHAM-280623/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a student to arbitrarily access and modify another student's personal notes. **CVE ID : CVE-2023-34962**	lms/commit/f9a17bfaf05994383bca5f4b65eb6897acc60d41, https://github.com/chamilo/chamilo-lms/commit/19af444d2da9e5a60f02b4ebe7755cdff36709cd	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jun-2023	6.1	Chamilo v1.11.x up to v1.11.18 was discovered to contain a cross-site scripting (XSS) vulnerability via the /feedback/comment field. **CVE ID : CVE-2023-34961**	https://support.chamilo.org/projects/1/wiki/Security_issues#Issue-105-2023-04-15-Low-impact-Moderate-risk-XSS-in-student-work-comments, https://github.com/chamilo/chamilo-lms/commit/80d1a8c9063a20f286b0195ef537c84a1a11875a	A-CHA-CHAM-280623/57
Server-Side Request Forgery (SSRF)	08-Jun-2023	5.3	An issue in Chamilo v1.11.* up to v1.11.18 allows attackers to execute a Server-Side Request Forgery (SSRF) and obtain information on the services running on the server via crafted	https://support.chamilo.org/projects/1/wiki/Security_issues#Issue-111-2023-04-20-Moderate-impact-Low-risk-Multiple-blind-SSRF-	A-CHA-CHAM-280623/58

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests in the social and links tools. **CVE ID : CVE-2023-34959**	in-links-and-social-tools, https://github.com/chamilo/chamilo-lms/commit/ed946908fef23e8aa4cefc28f745f3cd6710099f	
N/A	08-Jun-2023	4.3	Incorrect access control in Chamilo 1.11.* up to 1.11.18 allows a student subscribed to a given course to download documents belonging to another student if they know the document's ID. **CVE ID : CVE-2023-34958**	https://support.chamilo.org/projects/1/wiki/Security_issues#Issue-109-2023-04-15-Moderate-impact-Moderate-risk-IDOR-in-workstudent-publication, https://github.com/chamilo/chamilo-lms/commit/0c1c29db18856a6f25e21d0405dda2c20b35ff3a	A-CHA-CHAM-280623/59
Vendor: contec					
Product: conprosys_hmi_system					
Affected Version(s): * Up to (excluding) 3.5.3					
N/A	01-Jun-2023	8.8	Improper access control vulnerability exists in CONPROSYS HMI System (CHS) versions prior to 3.5.3. A user of the PC where the affected product is installed may gain an administrative	https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_s	A-CON-CONP-280623/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege. As a result, information regarding the product may be obtained and/or altered by the user. **CVE ID : CVE-2023-28657**	ecurity_chs_230531_jp.pdf, https://www.contec.com/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_chs_230531_en.pdf	
Cleartext Storage of Sensitive Information	01-Jun-2023	8.1	Plaintext storage of a password exists in CONPROSYS HMI System (CHS) versions prior to 3.5.3. Because account information of the database is saved in a local file in plaintext, a user who can access the PC where the affected product is installed can obtain the information. As a result, information in the database may be obtained and/or altered by the user. **CVE ID : CVE-2023-28713**	https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_chs_230531_jp.pdf, https://www.contec.com/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_chs_230531_en.pdf	A-CON-CONP-280623/61
Incorrect Permission Assignment for Critical Resource	01-Jun-2023	7.8	Incorrect permission assignment for critical resource exists in CONPROSYS HMI System (CHS) versions prior to 3.5.3. ACL (Access Control List) is not appropriately	https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-	A-CON-CONP-280623/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			set to the local folder where the affected product is installed, therefore a wide range of privileges is permitted to a user of the PC where the affected product is installed. As a result, the user may be able to destroy the system and/or execute a malicious program. **CVE ID : CVE-2023-28399**	info/contec_security_chs_230531_jp.pdf, https://www.contec.com/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_chs_230531_en.pdf	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Jun-2023	7.2	SQL injection vulnerability exists in the CONPROSYS HMI System (CHS) versions prior to 3.5.3. A user who can access the affected product with an administrative privilege may execute an arbitrary SQL command via specially crafted input to the query setting page. **CVE ID : CVE-2023-29154**	https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_chs_230531_jp.pdf, https://www.contec.com/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_chs_230531_en.pdf	A-CON-CONP-280623/63
Server-Side Request Forgery (SSRF)	01-Jun-2023	4.9	Server-side request forgery vulnerability exists in CONPROSYS HMI System (CHS) versions prior to 3.5.3. A user who can access	https://www.contec.com/jp/api/downloadlogger?download=/-/media/Conte	A-CON-CONP-280623/64

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected product with an administrative privilege may bypass the database restriction set on the query setting page, and connect to a user unintended database. **CVE ID : CVE-2023-28824**	c/jp/support/security-info/contec_security_chs_230531_jp.pdf, https://www.contec.com/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_chs_230531_en.pdf	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-2023	4.8	Cross-site scripting vulnerability exists in CONPROSYS HMI System (CHS) versions prior to 3.5.3. If a user who can access the affected product with an administrative privilege configures specially crafted settings, an arbitrary script may be executed on the web browser of the other user who is accessing the affected product with an administrative privilege. **CVE ID : CVE-2023-28651**	https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_chs_230531_jp.pdf, https://www.contec.com/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_chs_230531_en.pdf	A-CON-CONP-280623/65
Vendor: convertkit					
Product: convertkit_-_email_marketing\,_email_newsletter_and_landing_pages					
Affected Version(s): * Up to (excluding) 2.2.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2023	6.1	The ConvertKit WordPress plugin before 2.2.1 does not escape a parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-2337**	N/A	A-CON-CONV-280623/66
Vendor: corebos					
Product: corebos					
Affected Version(s): * Up to (excluding) 8.0					
Improper Authentication	02-Jun-2023	9.8	Unverified Password Change in GitHub repository tsolucio/corebos prior to 8. **CVE ID : CVE-2023-3069**	https://github.com/tsolucio/corebos/commit/e3dabd74c68646bb54538d66411fc1e633ec454b, https://huntr.dev/bounties/00544982-365a-476b-b5fe-42f02f11d367	A-COR-CORE-280623/67
Cross-Site Request Forgery (CSRF)	02-Jun-2023	6.5	Cross-Site Request Forgery (CSRF) in GitHub repository tsolucio/corebos prior to 8. **CVE ID : CVE-2023-3075**	https://huntr.dev/bounties/0f5448a6-d551-424f-887d-80f9bcfaa6e4, https://github.com/tsolucio/corebos/commit/2e415fb4613bc4122578dad5f40c	A-COR-CORE-280623/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				6f819c228a48	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository tsolucio/corebos prior to 8. **CVE ID : CVE-2023-3070**	https://huntr.dev/bounties/e193068e-0b95-403a-8453-e015241b8f1b, https://github.com/tsolucio/corebos/commit/b3a7a26c60117d7859b8d77b57fd5771a038c93a	A-COR-CORE-280623/69
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository tsolucio/corebos prior to 8. **CVE ID : CVE-2023-3073**	https://github.com/tsolucio/corebos/commit/e87f77c64061b43186c80ad1b50d313c67d7f6cf, https://huntr.dev/bounties/a4d6a082-2ea8-49a5-8e48-6d39b5cc62e1	A-COR-CORE-280623/70
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository tsolucio/corebos prior to 8. **CVE ID : CVE-2023-3074**	https://huntr.dev/bounties/6132f557-3f0f-465d-990f-4329313349a4, https://github.com/tsolucio/corebos/commit/659e328c06a127249	A-COR-CORE-280623/71

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				e651100d2bc7ec1d2dd8533	
Vendor: Dahuasecurity					
Product: smart_parking_management					
Affected Version(s): * Up to (including) 2023-05-28					
Server-Side Request Forgery (SSRF)	06-Jun-2023	4.6	A vulnerability has been found in Dahua Smart Parking Management up to 20230528 and classified as problematic. This vulnerability affects unknown code of the file /ipms/imageConvert/image. The manipulation of the argument fileUrl leads to server-side request forgery. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-230800. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3121**	N/A	A-DAH-SMAR-280623/72
Vendor: dataease					
Product: dataease					
Affected Version(s): * Up to (excluding) 1.18.7					
Deserialization of Untrusted Data	01-Jun-2023	9.8	DataEase is an open source data visualization and analysis tool. Prior to	https://github.com/dataease/dataease/security/advis	A-DAT-DATA-280623/73

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 1.18.7, a deserialization vulnerability exists in the DataEase datasource, which can be exploited to execute arbitrary code. The vulnerability has been fixed in v1.18.7. There are no known workarounds aside from upgrading. **CVE ID : CVE-2023-33963**	ories/GHSA-m26j-gh4m-xh9f	
Authorization Bypass Through User-Controlled Key	01-Jun-2023	8.1	DataEase is an open source data visualization and analysis tool. The API interface for DataEase delete dashboard and delete system messages is vulnerable to insecure direct object references (IDOR). This could result in a user deleting another user's dashboard or messages or interfering with the interface for marking messages read. The vulnerability has been fixed in v1.18.7. There are no known workarounds aside from upgrading. **CVE ID : CVE-2023-32310**	https://github.com/dataease/dataease/commit/72f428e87b5395c03d2f94ef6185fc247ddbc8dc, https://github.com/dataease/dataease/security/advisories/GHSA-7hv6-gv38-78wj, https://github.com/dataease/dataease/pull/5342	A-DAT-DATA-280623/74
Vendor: Dell					
Product: secure_connect_gateway					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 5.14.00.16					
Use of a Broken or Risky Cryptographic Algorithm	01-Jun-2023	6.5	Dell SCG 5.14 contains an information disclosure vulnerability during the SRS to SCG upgrade path. A remote low privileged malicious user could potentially exploit this vulnerability to retrieve the plain text. **CVE ID : CVE-2023-28043**	https://www.dell.com/support/kbdoc/en-us/000214205/dsa-2023-164-dell-secure-connect-gateway-security-update-for-multiple-vulnerabilities	A-DEL-SECU-280623/75
Vendor: deltaww					
Product: cncsoft-b					
Affected Version(s): * Up to (including) 1.0.0.4					
Out-of-bounds Write	07-Jun-2023	7.8	Delta Electronics' CNCSoft-B DOPSoft versions 1.0.0.4 and prior are vulnerable to heap-based buffer overflow, which could allow an attacker to execute arbitrary code. **CVE ID : CVE-2023-24014**	https://www.cisa.gov/news-events/ics-advisories/icsa-23-157-01	A-DEL-CNCS-280623/76
Stack-based Buffer Overflow	07-Jun-2023	7.8	Delta Electronics' CNCSoft-B DOPSoft	https://www.cisa.gov/news-events/ics-advisories/icsa-23-157-01	A-DEL-CNCS-280623/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 1.0.0.4 and prior are vulnerable to stack-based buffer overflow, which could allow an attacker to execute arbitrary code. **CVE ID : CVE-2023-25177**		
Vendor: diagrams					
Product: drawio					
Affected Version(s): * Up to (excluding) 21.2.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-2023	6.1	Cross-site Scripting (XSS) - Stored in GitHub repository jgraph/drawio prior to 21.2.8. **CVE ID : CVE-2023-3026**	https://github.com/jgraph/drawio/commit/c7ac634055c3edfabc7729fc4298a5ab7bfbf384, https://huntr.dev/bounties/9bbcc127-1e69-4c88-b318-d2afef48eff0	A-DIA-DRAW-280623/78
Vendor: dmtf					
Product: libspdm					
Affected Version(s): * Up to (excluding) 2.3.3					
N/A	01-Jun-2023	7.5	libspdm is a sample implementation that follows the DMTF SPDM specifications. Prior to versions 2.3.3 and 3.0, following a successful CAPABILITIES response, a libspdm	https://github.com/DMTF/libspdm/pull/2069, https://github.com/DMTF/libspdm/issues/2068, https://githu	A-DMT-LIBS-280623/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Requester stores the Responder's CTExponent into its context without validation. If the Requester sends a request message that requires a cryptography operation by the Responder, such as CHALLENGE, libspdm will calculate the timeout value using the Responder's unvalidated CTExponent. A patch is available in version 2.3.3. A workaround is also available. After completion of VCA, the Requester can check the value of the Responder's CTExponent. If it greater than or equal to 64, then the Requester can stop communication with the Responder. **CVE ID : CVE-2023-32690**	b.com/DMTF/libspdm/security/advisories/GHSA-56h8-4gv5-jf2c	
Vendor: Dokuwiki					
Product: dokuwiki					
Affected Version(s): * Up to (excluding) 2023-04-04a					
Improper Neutralization of Input During	05-Jun-2023	5.4	DokuWiki before 2023-04-04a allows XSS via RSS titles.	https://github.com/dokuwiki/dokuwiki/pull/3967, https://www.	A-DOK-DOKU-280623/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2023-34408**	github.com/splitbrain/dokuwiki/commit/53df38b0e4465894a67a5890f74a6f5f82e827de, https://github.com/dokuwiki/dokuwiki/compare/release-2023-04-04...release-2023-04-04a	
Vendor: don8_project					
Product: don8					
Affected Version(s): * Up to (including) 0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Kyle Maurer Don8 plugin <= 0.4 versions. **CVE ID : CVE-2023-32582**	N/A	A-DON-DON8-280623/81
Vendor: dottie_project					
Product: dottie					
Affected Version(s): * Up to (excluding) 2.0.4					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	10-Jun-2023	7.5	Versions of the package dottie before 2.0.4 are vulnerable to Prototype Pollution due to insufficient checks, via the set() function and the current variable in the /dottie.js file. **CVE ID : CVE-2023-26132**	https://github.com/mickhansen/dottie.js/commit/7d3aee1c9c3c842720506e131de7e181e5c8db68	A-DOT-DOTT-280623/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Draytek					
Product: myvigor					
Affected Version(s): * Up to (excluding) 2.3.2					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	A-DRA-MYVI-280623/83
Vendor: ebewe					
Product: city_autocomplete					
Affected Version(s): * Up to (excluding) 1.8.12					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	SQL injection vulnerability in the City Autocomplete (cityautocomplete) module from ebewe.net for PrestaShop, prior to version 1.8.12 (for PrestaShop version 1.5/1.6) or prior to 2.0.3 (for PrestaShop	N/A	A-EBE-CITY-280623/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 1.7), allows remote attackers to execute arbitrary SQL commands via the type, input_name. or q parameter in the autocompletion.php front controller. **CVE ID : CVE-2023-30149**		
Affected Version(s): * Up to (excluding) 2.0.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	SQL injection vulnerability in the City Autocomplete (cityautocomplete) module from ebewe.net for PrestaShop, prior to version 1.8.12 (for PrestaShop version 1.5/1.6) or prior to 2.0.3 (for PrestaShop version 1.7), allows remote attackers to execute arbitrary SQL commands via the type, input_name. or q parameter in the autocompletion.php front controller. **CVE ID : CVE-2023-30149**	N/A	A-EBE-CITY-280623/85
Vendor: elementor					
Product: elementor_pro					
Affected Version(s): * Up to (excluding) 3.11.7					
N/A	07-Jun-2023	8.8	The Elementor Pro plugin for WordPress is vulnerable to unauthorized data modification due to a missing capability	N/A	A-ELE-ELEM-280623/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check on the update_page_option function in versions up to, and including, 3.11.6. This makes it possible for authenticated attackers with subscriber-level capabilities to update arbitrary site options, which can lead to privilege escalation. **CVE ID : CVE-2023-3124**		
Vendor: elite					
Product: webfax					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	ELITE TECHNOLOGY CORP. Web Fax has a vulnerability of SQL Injection. An unauthenticated remote attacker can inject SQL commands into the input field of the login page to perform arbitrary system commands, disrupt service or terminate service. **CVE ID : CVE-2023-28701**	N/A	A-ELI-WEBF-280623/87
Vendor: Emoncms					
Product: emoncms					
Affected Version(s): 11.0					
Exposure of Resource	05-Jun-2023	5.3	emoncms v11 and later was discovered to contain an information disclosure vulnerability which	N/A	A-EMO-EMON-280623/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			allows attackers to obtain the web directory path and other information leaked by the server via a crafted web request. **CVE ID : CVE-2023-33518**		
Vendor: emqx					
Product: nanomq					
Affected Version(s): 0.17.2					
Use After Free	08-Jun-2023	7.5	A use-after-free vulnerability exists in NanoMQ 0.17.2. The vulnerability can be triggered by calling the function nni_mqtt_msg_get_publish_property() in the file mqtt_msg.c. This vulnerability is caused by improper data tracing, and an attacker could exploit it to cause a denial of service attack. **CVE ID : CVE-2023-33657**	https://github.com/emqx/nanomq/pull/1187	A-EMQ-NANO-280623/89
Out-of-bounds Write	08-Jun-2023	7.5	A heap buffer overflow vulnerability exists in NanoMQ 0.17.2. The vulnerability can be triggered by calling the function nni_msg_get_pub_pid() in the file message.c. An attacker could exploit this vulnerability to cause	https://github.com/nanomq/NanoNNG/commit/657e6c81c474bdee0e6413483b990e90610030c1	A-EMQ-NANO-280623/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial of service attack. **CVE ID : CVE-2023-33658**		
Out-of-bounds Write	06-Jun-2023	7.5	A heap buffer overflow vulnerability exists in NanoMQ 0.17.2. The vulnerability can be triggered by calling the function nmq_subinfo_decode() in the file mqtt_parser.c. An attacker could exploit this vulnerability to cause a denial of service attack. **CVE ID : CVE-2023-33659**	https://github.com/nanomq/NanoNNG/pull/509/commits/6815c4036a2344865da393803ecdb7af27d8bde1	A-EMQ-NANO-280623/91
Out-of-bounds Write	08-Jun-2023	7.5	A heap buffer overflow vulnerability exists in NanoMQ 0.17.2. The vulnerability can be triggered by calling the function copyn_str() in the file mqtt_parser.c. An attacker could exploit this vulnerability to cause a denial of service attack. **CVE ID : CVE-2023-33660**	https://github.com/nanomq/NanoNNG/pull/509/commits/6815c4036a2344865da393803ecdb7af27d8bde1	A-EMQ-NANO-280623/92
Affected Version(s): 0.17.5					
Out-of-bounds Write	12-Jun-2023	7.8	NanoMQ 0.17.5 is vulnerable to heap-buffer-overflow in the conn_handler function of mqtt_parser.c when	https://github.com/emqx/nanomq/issues/1181	A-EMQ-NANO-280623/93

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it processes malformed messages. **CVE ID : CVE-2023-34488**		
Vendor: encode					
Product: starlette					
Affected Version(s): From (including) 0.13.5 Up to (excluding) 0.27.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Jun-2023	7.5	Directory traversal vulnerability in Starlette versions 0.13.5 and later and prior to 0.27.0 allows a remote unauthenticated attacker to view files in a web service which was built using Starlette. **CVE ID : CVE-2023-29159**	https://github.com/encode/starlette/security/advisories/GHSA-v5gw-mw7f-84px	A-ENC-STAR-280623/94
Vendor: erikogluteknoloji					
Product: energy_monitoring					
Affected Version(s): * Up to (excluding) 230602					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Erikoglu Technology ErMon allows Command Line Execution through SQL Injection, Authentication Bypass.This issue affects ErMon: before 230602.	N/A	A-ERI-ENER-280623/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3000		
Vendor: erofs-utils_project					
Product: erofs-utils					
Affected Version(s): 1.6					
Out-of-bounds Write	01-Jun-2023	7.8	Heap Buffer Overflow in the erofsfsck_dirent_iter function in fsck/main.c in erofs-utils v1.6 allows remote attackers to execute arbitrary code via a crafted erofs filesystem image. **CVE ID : CVE-2023-33551**	https://github.com/lometsj/blog_repo/issues/2	A-ERO-EROF-280623/96
Out-of-bounds Write	01-Jun-2023	7.8	Heap Buffer Overflow in the erofs_read_one_data function at data.c in erofs-utils v1.6 allows remote attackers to execute arbitrary code via a crafted erofs filesystem image. **CVE ID : CVE-2023-33552**	https://github.com/lometsj/blog_repo/issues/1	A-ERO-EROF-280623/97
Vendor: escanav					
Product: escan_management_console					
Affected Version(s): 14.0.1400.2281					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-2023	6.1	Reflected Cross Site Scripting (XSS) in the view dashboard detail feature in Microworld Technologies eScan management console 14.0.1400.2281 allows remote attacker to	N/A	A-ESC-ESCA-280623/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject arbitrary code via the URL directly. **CVE ID : CVE-2023-33731**		
Vendor: expresstech					
Product: quiz_and_survey_master					
Affected Version(s): * Up to (including) 8.0.8					
Missing Authorization	09-Jun-2023	9.1	The Quiz And Survey Master for WordPress is vulnerable to authorization bypass due to a missing capability check on the function associated with the qsm_remove_file_fd_question AJAX action in versions up to, and including, 8.0.8. This makes it possible for unauthenticated attackers to delete arbitrary media files. **CVE ID : CVE-2023-0291**	https://plugins.trac.wordpress.org/changeset/2834471/quiz-master-next	A-EXP-QUIZ-280623/99
Cross-Site Request Forgery (CSRF)	09-Jun-2023	8.1	The Quiz And Survey Master plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 8.0.8. This is due to missing nonce validation on the function associated with the qsm_remove_file_fd_question AJAX action. This makes it possible for unauthenticated attackers to delete arbitrary media files	https://plugins.trac.wordpress.org/changeset/2834471/quiz-master-next	A-EXP-QUIZ-280623/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-0292**		
Vendor: eyoucms					
Product: eyoucms					
Affected Version(s): 1.6.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jun-2023	5.4	EyouCMS 1.6.2 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-33492**	N/A	A-EYO-EYOU-280623/101
Vendor: faculty_evaluation_system_project					
Product: faculty_evaluation_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	06-Jun-2023	7.2	Sourcecodester Faculty Evaluation System v1.0 is vulnerable to arbitrary code execution via ip/eval/ajax.php?action=update_user. **CVE ID : CVE-2023-33569**	N/A	A-FAC-FACU-280623/102
Vendor: fast-xml-parser_project					
Product: fast-xml-parser					
Affected Version(s): * Up to (excluding) 4.2.4					
N/A	06-Jun-2023	7.5	fast-xml-parser is an open source, pure javascript xml parser.	https://github.com/NaturalIntelligence/f	A-FAS-FAST-280623/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fast-xml-parser allows special characters in entity names, which are not escaped or sanitized. Since the entity name is used for creating a regex for searching and replacing entities in the XML body, an attacker can abuse it for denial of service (DoS) attacks. By crafting an entity name that results in an intentionally bad performing regex and utilizing it in the entity replacement step of the parser, this can cause the parser to stall for an indefinite amount of time. This problem has been resolved in v4.2.4. Users are advised to upgrade. Users unable to upgrade should avoid using DOCTYPE parsing by setting the `processEntities: false` option. **CVE ID : CVE-2023-34104**	ast-xml-parser/security/advisories/GHSA-6w63-h3fj-q4vw, https://github.com/NaturalIntelligence/fast-xml-parser/commit/39b0e050bb909e8499478657f84a3076e39ce76c	
Vendor: fibosearch					
Product: fibosearch					
Affected Version(s): * Up to (including) 1.23.0					
Improper Neutralization of Input During	09-Jun-2023	4.4	The FiboSearch - AJAX Search for WooCommerce plugin for WordPress is vulnerable to Stored	https://plugins.trac.wordpress.org/changeset?old_path=%2Fajax-	A-FIB-FIBO-280623/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Cross-Site Scripting via admin settings in versions up to, and including, 1.23.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-2450**	search-for-woocommerce%2Ftags%2F1.23.0&old=2917453&new_path=%2Fajax-search-for-woocommerce%2Ftags%2F1.24.0&new=2917453&sfp_email=&sfph_mail=	
Vendor: Froxlor					
Product: froxlor					
Affected Version(s): * Up to (excluding) 2.0.20					
Improper Restriction of Excessive Authentication Attempts	09-Jun-2023	9.8	Improper Restriction of Excessive Authentication Attempts in GitHub repository froxlor/froxlor prior to 2.0.20. **CVE ID : CVE-2023-3173**	https://github.com/froxlor/froxlor/commit/464216072456efb35b4541c58e7016463dfbd9a6, https://huntr.dev/bounties/4d715f76-950d-4251-8139-3dffea798f14	A-FRO-FROX-280623/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Jun-2023	7.2	Path Traversal in GitHub repository froxlor/froxlor prior to 2.0.20. **CVE ID : CVE-2023-3172**	https://huntr.dev/bounties/e50966cd-9222-46b9-aedc-1feb3f2a0b0e, https://github.com/froxlor/froxlor/commit/da810ea95393dfaec68a70e30b7c887c50563a7e	A-FRO-FROX-280623/106
Affected Version(s): * Up to (excluding) 2.1.0					
Session Fixation	11-Jun-2023	5.4	Session Fixation in GitHub repository froxlor/froxlor prior to 2.1.0. **CVE ID : CVE-2023-3192**	https://huntr.dev/bounties/f3644772-9c86-4f55-a0fa-aeb11f411551, https://github.com/froxlor/froxlor/commit/94d9c3eedf31bc8447e3aa349e32880dde02ee52	A-FRO-FROX-280623/107
Vendor: getshieldsecurity					
Product: shield_security					
Affected Version(s): * Up to (including) 17.0.17					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	6.1	The Shield Security plugin for WordPress is vulnerable to stored Cross-Site Scripting in versions up to, and including, 17.0.17 via the 'User-Agent' header. This makes it possible for unauthenticated attackers to inject	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2883864%40wp-simple-firewall%2Ftrunk&old=288	A-GET-SHIE-280623/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-0992**	3536%40wp-simple-firewall%2Ftrunk&sfp_email=&sfph_mail=	
Missing Authorization	09-Jun-2023	4.3	The Shield Security plugin for WordPress is vulnerable to Missing Authorization on the 'theme-plugin-file' AJAX action in versions up to, and including, 17.0.17. This allows authenticated attackers to add arbitrary audit log entries indicating that a theme or plugin has been edited, and is also a vector for Cross-Site Scripting via CVE-2023-0992. **CVE ID : CVE-2023-0993**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2883864%40wp-simple-firewall%2Ftrunk&old=2883536%40wp-simple-firewall%2Ftrunk&sfp_email=&sfph_mail=	A-GET-SHIE-280623/109
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): * Up to (excluding) 15.10.8					
N/A	07-Jun-2023	4.3	An issue has been discovered in GitLab CE/EE affecting all versions before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. An attacker was able to spoof protected tags, which could	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2001.json	A-GIT-GITL-280623/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially lead a victim to download malicious code. **CVE ID : CVE-2023-2001**		
Affected Version(s): From (including) 1.2.0 Up to (excluding) 15.10.8					
N/A	07-Jun-2023	4.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 1.2 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. An issue was found that allows someone to abuse a discrepancy between the Web application display and the git command line interface to social engineer victims into cloning non-trusted code. **CVE ID : CVE-2023-2013**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2013.json	A-GIT-GITL-280623/111
Affected Version(s): From (including) 12.0.0 Up to (excluding) 15.10.5					
N/A	06-Jun-2023	6.5	An issue has been discovered in GitLab EE affecting all versions starting from 12.0 before 15.10.5, all versions starting from 15.11 before 15.11.1. A malicious group member may continue to commit to projects even from a restricted IP address.	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1621.json, https://gitlab.com/gitlab-org/gitlab/-/issues/399774	A-GIT-GITL-280623/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1621		
Affected Version(s): From (including) 12.0.0 Up to (excluding) 15.10.8					
N/A	07-Jun-2023	7.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.0 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A Regular Expression Denial of Service was possible via sending crafted payloads to the preview_markdown endpoint. **CVE ID : CVE-2023-2199**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2199.json	A-GIT-GITL-280623/113
N/A	07-Jun-2023	5.3	An issue has been discovered in GitLab EE affecting all versions starting from 12.0 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. An attacker can clone a repository from a public project, from a disallowed IP, even after the top-level group has enabled IP restrictions on the group. **CVE ID : CVE-2023-2589**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2589.json	A-GIT-GITL-280623/114
Affected Version(s): From (including) 13.2.4 Up to (excluding) 15.10.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	07-Jun-2023	7.5	A denial of service issue was discovered in GitLab CE/EE affecting all versions starting from 13.2.4 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2 which allows an attacker to cause high resource consumption using malicious test report artifacts. **CVE ID : CVE-2023-0121**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0121.json	A-GIT-GITL-280623/115
Affected Version(s): From (including) 14.1.0 Up to (excluding) 15.10.8					
Improper Privilege Management	07-Jun-2023	4.9	An issue has been discovered in GitLab CE/EE affecting all versions starting from 14.1 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A malicious maintainer in a project can escalate other users to Owners in that project if they import members from another project that those other users are Owners of. **CVE ID : CVE-2023-2485**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2485.json	A-GIT-GITL-280623/116
Affected Version(s): From (including) 15.11.0 Up to (excluding) 15.11.1					
N/A	06-Jun-2023	6.5	An issue has been discovered in GitLab EE affecting all	https://gitlab.com/gitlab-org/cves/-	A-GIT-GITL-280623/117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions starting from 12.0 before 15.10.5, all versions starting from 15.11 before 15.11.1. A malicious group member may continue to commit to projects even from a restricted IP address. **CVE ID : CVE-2023-1621**	/blob/master/2023/CVE-2023-1621.json, https://gitlab.com/gitlab-org/gitlab/-/issues/399774	
Affected Version(s): From (including) 15.11.0 Up to (excluding) 15.11.7					
Uncontrolled Resource Consumption	07-Jun-2023	7.5	A denial of service issue was discovered in GitLab CE/EE affecting all versions starting from 13.2.4 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2 which allows an attacker to cause high resource consumption using malicious test report artifacts. **CVE ID : CVE-2023-0121**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0121.json	A-GIT-GITL-280623/118
N/A	06-Jun-2023	7.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.4 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A DollarMathPostFilter Regular Expression Denial of Service in	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2132.json	A-GIT-GITL-280623/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was possible by sending crafted payloads to the preview_markdown endpoint. **CVE ID : CVE-2023-2132**		
N/A	07-Jun-2023	7.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 8.7 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A Regular Expression Denial of Service was possible via sending crafted payloads to the preview_markdown endpoint. **CVE ID : CVE-2023-2198**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2198.json	A-GIT-GITL-280623/120
N/A	07-Jun-2023	7.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.0 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A Regular Expression Denial of Service was possible via sending crafted payloads to the preview_markdown endpoint.	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2199.json	A-GIT-GITL-280623/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2199		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2023	6.1	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.8 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A reflected XSS was possible when creating new abuse reports which allows attackers to perform arbitrary actions on behalf of victims. **CVE ID : CVE-2023-2015**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2015.json	A-GIT-GITL-280623/122
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2023	5.4	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A specially crafted merge request could lead to a stored XSS on the client side which allows attackers to perform arbitrary actions on behalf of victims. **CVE ID : CVE-2023-2442**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2442.json	A-GIT-GITL-280623/123
N/A	07-Jun-2023	5.3	An issue has been discovered in GitLab EE affecting all versions starting from 12.0 before 15.10.8, all	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-	A-GIT-GITL-280623/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. An attacker can clone a repository from a public project, from a disallowed IP, even after the top-level group has enabled IP restrictions on the group. **CVE ID : CVE-2023-2589**	2023-2589.json	
Improper Privilege Management	07-Jun-2023	4.9	An issue has been discovered in GitLab CE/EE affecting all versions starting from 14.1 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A malicious maintainer in a project can escalate other users to Owners in that project if they import members from another project that those other users are Owners of. **CVE ID : CVE-2023-2485**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2485.json	A-GIT-GITL-280623/125
N/A	07-Jun-2023	4.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.4 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0508.json	A-GIT-GITL-280623/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.0.2. Open redirection was possible via HTTP response splitting in the NPM package API. **CVE ID : CVE-2023-0508**		
Uncontrolled Resource Consumption	06-Jun-2023	4.3	A lack of length validation in GitLab CE/EE affecting all versions from 8.3 before 15.10.8, 15.11 before 15.11.7, and 16.0 before 16.0.2 allows an authenticated attacker to create a large Issue description via GraphQL which, when repeatedly requested, saturates CPU usage. **CVE ID : CVE-2023-0921**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0921.json	A-GIT-GITL-280623/127
Exposure of Resource to Wrong Sphere	07-Jun-2023	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 15.7 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. It was possible to disclose issue notes to an unauthorized user at project export. **CVE ID : CVE-2023-1825**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1825.json	A-GIT-GITL-280623/128
N/A	07-Jun-2023	4.3	An issue has been discovered in GitLab CE/EE affecting all versions before	https://gitlab.com/gitlab-org/cves/-/blob/master	A-GIT-GITL-280623/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. An attacker was able to spoof protected tags, which could potentially lead a victim to download malicious code. **CVE ID : CVE-2023-2001**	/2023/CVE-2023-2001.json	
N/A	07-Jun-2023	4.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 1.2 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. An issue was found that allows someone to abuse a discrepancy between the Web application display and the git command line interface to social engineer victims into cloning non-trusted code. **CVE ID : CVE-2023-2013**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2013.json	A-GIT-GITL-280623/130
Affected Version(s): From (including) 15.4.0 Up to (excluding) 15.10.8					
N/A	06-Jun-2023	7.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.4 before 15.10.8, all versions starting from	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-	A-GIT-GITL-280623/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A DollarMathPostFilter Regular Expression Denial of Service in was possible by sending crafted payloads to the preview_markdown endpoint. **CVE ID : CVE-2023-2132**	2023-2132.json	
N/A	07-Jun-2023	4.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.4 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. Open redirection was possible via HTTP response splitting in the NPM package API. **CVE ID : CVE-2023-0508**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0508.json	A-GIT-GITL-280623/132
Affected Version(s): From (including) 15.7.0 Up to (excluding) 15.10.8					
Exposure of Resource to Wrong Sphere	07-Jun-2023	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 15.7 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. It was possible to disclose issue notes	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1825.json	A-GIT-GITL-280623/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to an unauthorized user at project export. **CVE ID : CVE-2023-1825**		
Affected Version(s): From (including) 15.8.0 Up to (excluding) 15.10.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2023	6.1	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.8 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A reflected XSS was possible when creating new abuse reports which allows attackers to perform arbitrary actions on behalf of victims. **CVE ID : CVE-2023-2015**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2015.json	A-GIT-GITL-280623/134
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.0.2					
Uncontrolled Resource Consumption	07-Jun-2023	7.5	A denial of service issue was discovered in GitLab CE/EE affecting all versions starting from 13.2.4 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2 which allows an attacker to cause high resource consumption using malicious test report artifacts. **CVE ID : CVE-2023-0121**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0121.json	A-GIT-GITL-280623/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Jun-2023	7.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.4 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A DollarMathPostFilter Regular Expression Denial of Service in was possible by sending crafted payloads to the preview_markdown endpoint. **CVE ID : CVE-2023-2132**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2132.json	A-GIT-GITL-280623/136
N/A	07-Jun-2023	7.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 8.7 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A Regular Expression Denial of Service was possible via sending crafted payloads to the preview_markdown endpoint. **CVE ID : CVE-2023-2198**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2198.json	A-GIT-GITL-280623/137
N/A	07-Jun-2023	7.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.0 before 15.10.8, all	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-	A-GIT-GITL-280623/138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A Regular Expression Denial of Service was possible via sending crafted payloads to the preview_markdown endpoint. **CVE ID : CVE-2023-2199**	2023-2199.json	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2023	6.1	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.8 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A reflected XSS was possible when creating new abuse reports which allows attackers to perform arbitrary actions on behalf of victims. **CVE ID : CVE-2023-2015**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2015.json	A-GIT-GITL-280623/139
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2023	5.4	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A specially crafted merge request could lead to a stored XSS on the client side which allows	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2442.json	A-GIT-GITL-280623/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to perform arbitrary actions on behalf of victims. **CVE ID : CVE-2023-2442**		
N/A	07-Jun-2023	5.3	An issue has been discovered in GitLab EE affecting all versions starting from 12.0 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. An attacker can clone a repository from a public project, from a disallowed IP, even after the top-level group has enabled IP restrictions on the group. **CVE ID : CVE-2023-2589**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2589.json	A-GIT-GITL-280623/141
Improper Privilege Management	07-Jun-2023	4.9	An issue has been discovered in GitLab CE/EE affecting all versions starting from 14.1 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A malicious maintainer in a project can escalate other users to Owners in that project if they import members from another project that those other users are Owners of.	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2485.json	A-GIT-GITL-280623/142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2485		
N/A	07-Jun-2023	4.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.4 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. Open redirection was possible via HTTP response splitting in the NPM package API. **CVE ID : CVE-2023-0508**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0508.json	A-GIT-GITL-280623/143
Uncontrolled Resource Consumption	06-Jun-2023	4.3	A lack of length validation in GitLab CE/EE affecting all versions from 8.3 before 15.10.8, 15.11 before 15.11.7, and 16.0 before 16.0.2 allows an authenticated attacker to create a large Issue description via GraphQL which, when repeatedly requested, saturates CPU usage. **CVE ID : CVE-2023-0921**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0921.json	A-GIT-GITL-280623/144
Exposure of Resource to Wrong Sphere	07-Jun-2023	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 15.7 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1825.json	A-GIT-GITL-280623/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from 16.0 before 16.0.2. It was possible to disclose issue notes to an unauthorized user at project export. **CVE ID : CVE-2023-1825**		
N/A	07-Jun-2023	4.3	An issue has been discovered in GitLab CE/EE affecting all versions before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. An attacker was able to spoof protected tags, which could potentially lead a victim to download malicious code. **CVE ID : CVE-2023-2001**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2001.json	A-GIT-GITL-280623/146
N/A	07-Jun-2023	4.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 1.2 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. An issue was found that allows someone to abuse a discrepancy between the Web application display and the git command line interface to social engineer victims into	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2013.json	A-GIT-GITL-280623/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cloning non-trusted code. **CVE ID : CVE-2023-2013**		
Affected Version(s): From (including) 8.3.0 Up to (excluding) 15.10.8					
Uncontrolled Resource Consumption	06-Jun-2023	4.3	A lack of length validation in GitLab CE/EE affecting all versions from 8.3 before 15.10.8, 15.11 before 15.11.7, and 16.0 before 16.0.2 allows an authenticated attacker to create a large Issue description via GraphQL which, when repeatedly requested, saturates CPU usage. **CVE ID : CVE-2023-0921**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0921.json	A-GIT-GITL-280623/148
Affected Version(s): From (including) 8.7.0 Up to (excluding) 15.10.8					
N/A	07-Jun-2023	7.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 8.7 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A Regular Expression Denial of Service was possible via sending crafted payloads to the preview_markdown endpoint. **CVE ID : CVE-2023-2198**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2198.json	A-GIT-GITL-280623/149
Vendor: gitpod					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: gitpod					
Affected Version(s): * Up to (excluding) 2022.11.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2023	6.1	Gitpod before 2022.11.3 allows XSS because redirection can occur for some protocols outside of the trusted set of three (vscode: vscode-insiders: jetbrains-gateway:). **CVE ID : CVE-2023-32766**	https://github.com/gitpod-io/gitpod/pull/17559, https://github.com/gitpod-io/gitpod/compare/release-2022.11.2...2022.11.3, https://github.com/gitpod-io/gitpod/commit/6771283c3406586e352337675b79ff2ca50f191b	A-GIT-GITP-280623/150
Vendor: glitter_unicorn_wallpaper_project					
Product: glitter_unicorn_wallpaper					
Affected Version(s): From (including) 7.0 Up to (including) 8.0					
N/A	01-Jun-2023	9.1	The Glitter Unicorn Wallpaper app for Android 7.0 thru 8.0 allows unauthorized apps to actively request permission to modify data in the database that records information about a user's personal preferences and will be loaded into memory to be read and used when the app is opened. An attacker could tamper with this data to cause an escalation of privilege attack.	N/A	A-GLI-GLIT-280623/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29722		
N/A	01-Jun-2023	7.5	The Glitter Unicorn Wallpaper app for Android 7.0 thru 8.0 allows unauthorized applications to actively request permission to insert data into the database that records information about a user's personal preferences and will be loaded into memory to be read and used when the application is opened. By injecting data, the attacker can force the application to load malicious image URLs and display them in the UI. As the amount of data increases, it will eventually cause the application to trigger an OOM error and crash, resulting in a persistent denial of service attack. **CVE ID : CVE-2023-29723**	N/A	A-GLI-GLIT-280623/152
Vendor: Golang					
Product: go					
Affected Version(s): * Up to (excluding) 1.19.10					
Exposure of Resource to Wrong Sphere	08-Jun-2023	7.8	On Unix platforms, the Go runtime does not behave differently when a binary is run with the setuid/setgid bits. This can be	https://pkg.go.dev/vuln/GO-2023-1840, https://go.dev/cl/501223	A-GOL-GO-280623/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dangerous in certain cases, such as when dumping memory state, or assuming the status of standard i/o file descriptors. If a setuid/setgid binary is executed with standard I/O file descriptors closed, opening any files can result in unexpected content being read or written with elevated privileges. Similarly, if a setuid/setgid program is terminated, either via panic or signal, it may leak the contents of its registers. **CVE ID : CVE-2023-29403**		
Affected Version(s): From (including) 1.20.0 Up to (excluding) 1.20.5					
Exposure of Resource to Wrong Sphere	08-Jun-2023	7.8	On Unix platforms, the Go runtime does not behave differently when a binary is run with the setuid/setgid bits. This can be dangerous in certain cases, such as when dumping memory state, or assuming the status of standard i/o file descriptors. If a setuid/setgid binary is executed with standard I/O file descriptors closed, opening any files can result in unexpected content being read or	https://pkg.go.dev/vuln/GO-2023-1840, https://go.dev/cl/501223	A-GOL-GO-280623/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			written with elevated privileges. Similarly, if a setuid/setgid program is terminated, either via panic or signal, it may leak the contents of its registers. **CVE ID : CVE-2023-29403**		
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 114.0.5735.110					
Access of Resource Using Incompatible Type ('Type Confusion')	05-Jun-2023	8.8	Type confusion in V8 in Google Chrome prior to 114.0.5735.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-3079**	N/A	A-GOO-CHRO-280623/155
Vendor: gougucms					
Product: pythagorean_oa_office_system					
Affected Version(s): * Up to (including) 4.50.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-2023	5.4	A vulnerability has been found in Guangdong Pythagorean OA Office System up to 4.50.31 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Schedule Handler. The	N/A	A-GOU-PYTH-280623/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument description 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-230467. **CVE ID : CVE-2023-3035**		
Vendor: grafana					
Product: grafana					
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.5.26					
Missing Authorization	06-Jun-2023	6.4	Grafana is an open-source platform for monitoring and observability. The option to send a test alert is not available from the user panel UI for users having the Viewer role. It is still possible for a user with the Viewer role to send a test alert using the API as the API does not check access to this function. This might enable malicious users to abuse the functionality by sending multiple alert messages to e-mail	https://grafana.com/security/security-advisories/cve-2023-2183/	A-GRA-GRAF-280623/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Slack, spamming users, prepare Phishing attack or block SMTP server. Users may upgrade to version 9.5.3, 9.4.12, 9.3.15, 9.2.19 and 8.5.26 to receive a fix. **CVE ID : CVE-2023-2183**		
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.2.19					
Missing Authorization	06-Jun-2023	6.4	Grafana is an open-source platform for monitoring and observability. The option to send a test alert is not available from the user panel UI for users having the Viewer role. It is still possible for a user with the Viewer role to send a test alert using the API as the API does not check access to this function. This might enable malicious users to abuse the functionality by sending multiple alert messages to e-mail and Slack, spamming users, prepare	https://grafana.com/security/security-advisories/cve-2023-2183/	A-GRA-GRAF-280623/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Phishing attack or block SMTP server. Users may upgrade to version 9.5.3, 9.4.12, 9.3.15, 9.2.19 and 8.5.26 to receive a fix. **CVE ID : CVE-2023-2183**		
Affected Version(s): From (including) 9.3.0 Up to (excluding) 9.3.15					
Missing Authorization	06-Jun-2023	6.4	Grafana is an open-source platform for monitoring and observability. The option to send a test alert is not available from the user panel UI for users having the Viewer role. It is still possible for a user with the Viewer role to send a test alert using the API as the API does not check access to this function. This might enable malicious users to abuse the functionality by sending multiple alert messages to e-mail and Slack, spamming users, prepare Phishing attack or block SMTP server.	https://grafana.com/security/security-advisories/cve-2023-2183/	A-GRA-GRAF-280623/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Users may upgrade to version 9.5.3, 9.4.12, 9.3.15, 9.2.19 and 8.5.26 to receive a fix. **CVE ID : CVE-2023-2183**		
Affected Version(s): From (including) 9.4.0 Up to (excluding) 9.4.12					
Missing Authorization	06-Jun-2023	6.4	Grafana is an open-source platform for monitoring and observability. The option to send a test alert is not available from the user panel UI for users having the Viewer role. It is still possible for a user with the Viewer role to send a test alert using the API as the API does not check access to this function. This might enable malicious users to abuse the functionality by sending multiple alert messages to e-mail and Slack, spamming users, prepare Phishing attack or block SMTP server.	https://grafana.com/security/security-advisories/cve-2023-2183/	A-GRA-GRAF-280623/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Users may upgrade to version 9.5.3, 9.4.12, 9.3.15, 9.2.19 and 8.5.26 to receive a fix. **CVE ID : CVE-2023-2183**		
Improper Synchronization	06-Jun-2023	5.3	Grafana is an open-source platform for monitoring and observability. Using public dashboards users can query multiple distinct data sources using mixed queries. However such query has a possibility of crashing a Grafana instance. The only feature that uses mixed queries at the moment is public dashboards, but it's also possible to cause this by calling the query API directly. This might enable malicious users to crash Grafana instances through that endpoint. Users may upgrade to version 9.4.12 and 9.5.3 to receive a fix.	https://grafana.com/security/security-advisories/cve-2023-2801/	A-GRA-GRAF-280623/161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2801		
Affected Version(s): From (including) 9.5.0 Up to (excluding) 9.5.3					
Missing Authorization	06-Jun-2023	6.4	Grafana is an open-source platform for monitoring and observability. The option to send a test alert is not available from the user panel UI for users having the Viewer role. It is still possible for a user with the Viewer role to send a test alert using the API as the API does not check access to this function. This might enable malicious users to abuse the functionality by sending multiple alert messages to e-mail and Slack, spamming users, prepare Phishing attack or block SMTP server. Users may upgrade to version 9.5.3, 9.4.12, 9.3.15, 9.2.19 and 8.5.26 to receive a fix.	https://grafana.com/security/security-advisories/cve-2023-2183/	A-GRA-GRAF-280623/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2183		
Improper Synchronization	06-Jun-2023	5.3	Grafana is an open-source platform for monitoring and observability. Using public dashboards users can query multiple distinct data sources using mixed queries. However such query has a possibility of crashing a Grafana instance. The only feature that uses mixed queries at the moment is public dashboards, but it's also possible to cause this by calling the query API directly. This might enable malicious users to crash Grafana instances through that endpoint. Users may upgrade to version 9.4.12 and 9.5.3 to receive a fix. **CVE ID : CVE-2023-2801**	https://grafana.com/security/security-advisories/cve-2023-2801/	A-GRA-GRAF-280623/163
Vendor: Grpc					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: grpc					
Affected Version(s): * Up to (excluding) 1.53.0					
N/A	09-Jun-2023	5.3	gRPC contains a vulnerability whereby a client can cause a termination of connection between a HTTP2 proxy and a gRPC server: a base64 encoding error for `-bin` suffixed headers will result in a disconnection by the gRPC server, but is typically allowed by HTTP2 proxies. We recommend upgrading beyond the commit in https://github.com/grpc/grpc/pull/32309 https://www.google.com/url **CVE ID : CVE-2023-32732**	https://github.com/grpc/grpc/pull/32309	A-GRP-GRPC-280623/164
Affected Version(s): From (including) 1.51.0 Up to (excluding) 1.53.0					
Reachable Assertion	09-Jun-2023	7.5	There exists an vulnerability causing an abort() to be called in gRPC. The following headers cause gRPC's C++ implementation to abort() when called via http2: te: x (x != trailers)	https://github.com/grpc/grpc/commit/2485fa94bd8a723e5c977d55a3ce10b301b437f8	A-GRP-GRPC-280623/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			:scheme: x (x != http, https) grpclb_client_stats: x (x == anything) On top of sending one of those headers, a later header must be sent that gets the total header size past 8KB. We recommend upgrading past git commit 2485fa94bd8a723e5c977d55a3ce10b301b437f8 or v1.53 and above. **CVE ID : CVE-2023-1428**		
Affected Version(s): From (including) 1.53.0 Up to (excluding) 1.55.0					
N/A	09-Jun-2023	7.5	When gRPC HTTP2 stack raised a header size exceeded error, it skipped parsing the rest of the HPACK frame. This caused any HPACK table mutations to also be skipped, resulting in a desynchronization of HPACK tables between sender and receiver. If leveraged, say, between a proxy and a backend, this could lead to requests from the proxy being interpreted as containing headers	https://github.com/grpc/grpc/pull/32309, https://github.com/grpc/grpc/pull/33005	A-GRP-GRPC-280623/166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from different proxy clients - leading to an information leak that can be used for privilege escalation or data exfiltration. We recommend upgrading beyond the commit contained in https://github.com/grpc/grpc/pull/33005 https://github.com/grpc/grpc/pull/33005 **CVE ID : CVE-2023-32731**		
Vendor: harbingergroup					
Product: office_player					
Affected Version(s): 4.0.6.0.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jun-2023	7.5	OfflinePlayerService.exe in Harbinger Offline Player 4.0.6.0.2 allows directory traversal as LocalSystem via ..\ in a URL. **CVE ID : CVE-2023-34407**	N/A	A-HAR-OFFI-280623/167
Vendor: hashicorp					
Product: consul					
Affected Version(s): From (including) 1.13.0 Up to (excluding) 1.14.7					
N/A	02-Jun-2023	7.5	Consul and Consul Enterprise's cluster peering implementation contained a flaw whereby a peer cluster with service of the same name as a local service could	https://discuss.hashicorp.com/t/hcsec-2023-15-consul-cluster-peering-can-result-in-denial-of-	A-HAS-CONS-280623/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corrupt Consul state, resulting in denial of service. This vulnerability was resolved in Consul 1.14.5, and 1.15.3 **CVE ID : CVE-2023-1297**	service/54515	
Affected Version(s): From (including) 1.15.0 Up to (excluding) 1.15.3					
N/A	02-Jun-2023	7.5	Consul and Consul Enterprise's cluster peering implementation contained a flaw whereby a peer cluster with service of the same name as a local service could corrupt Consul state, resulting in denial of service. This vulnerability was resolved in Consul 1.14.5, and 1.15.3 **CVE ID : CVE-2023-1297**	https://discuss.hashicorp.com/t/hcsec-2023-15-consul-cluster-peering-can-result-in-denial-of-service/54515	A-HAS-CONS-280623/169
N/A	02-Jun-2023	6.5	Consul and Consul Enterprise allowed any user with service:write permissions to use Envoy extensions configured via service-defaults to patch remote proxy instances that target the configured service, regardless of whether the user has permission to modify the service(s) corresponding to	https://discuss.hashicorp.com/t/hcsec-2023-16-consul-envoy-extension-downstream-proxy-configuration-by-upstream-service-owner/54525	A-HAS-CONS-280623/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			those modified proxies. **CVE ID : CVE-2023-2816**		
Vendor: hawt					
Product: hawtio					
Affected Version(s): 2.17.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Jun-2023	5.5	hawtio 2.17.2 is vulnerable to Path Traversal. it is possible to input malicious zip files, which can result in the high-risk files after decompression being stored in any location, even leading to file overwrite. **CVE ID : CVE-2023-33544**	N/A	A-HAW-HAWT-280623/171
Vendor: hidglobal					
Product: safe					
Affected Version(s): From (including) 5.8.0 Up to (including) 5.11.3					
N/A	07-Jun-2023	7.3	The External Visitor Manager portal of HID's SAFE versions 5.8.0 through 5.11.3 are vulnerable to manipulation within web fields in the application programmable interface (API). An attacker could log in using account credentials available through a	https://www.hidglobal.com/security-center	A-HID-SAFE-280623/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request generated by an internal user and then manipulate the visitor-id within the web API to access the personal data of other users. There is no limit on the number of requests that can be made to the HID SAFE Web Server, so an attacker could also exploit this vulnerability to create a denial-of-service condition. **CVE ID : CVE-2023-2904**		
Vendor: hijiriworld					
Product: intuitive_custom_post_order					
Affected Version(s): * Up to (including) 3.1.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Jun-2023	7.2	The Intuitive Custom Post Order plugin for WordPress is vulnerable to SQL Injection in versions up to, and including, 3.1.3, due to insufficient escaping on the user supplied 'objects' and 'tags' parameters and lack of sufficient preparation in the 'update_options' function as well as the	https://plugins.trac.wordpress.org/browser/intuitive-custom-post-order/trunk/intuitive-custom-post-order.php?rev=2530122	A-HIJ-INTU-280623/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'refresh' function which runs queries on the same values. This allows authenticated attackers, with administrator permissions, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Note that this attack may only be practical on configurations where it is possible to bypass addslashes due to the database using a nonstandard character set such as GBK. **CVE ID : CVE-2023-1016**		
Vendor: hoppscotch					
Product: hoppscotch					
Affected Version(s): * Up to (excluding) 2023.4.5					
Insertion of Sensitive Information into Log File	05-Jun-2023	8.8	hoppscotch is an open source API development ecosystem. In versions prior to 2023.4.5 the database password is exposed in the logs when showing the database connection string. Attackers with access to read system logs will be able to elevate privilege with full access to the database. Users are	https://github.com/hoppscotch/hoppscotch/commit/15424903ede20b155d764abf4c4f7c2c84c11247, https://github.com/hoppscotch/hoppscotch/security/advisories/GHSA-qpx8-wq6q-r833	A-HOP-HOPP-280623/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-34097**		
Vendor: hornerautomation					
Product: cscape					
Affected Version(s): 9.90					
Out-of-bounds Read	06-Jun-2023	7.8	The affected application lacks proper validation of user-supplied data when parsing font files (e.g., FNT). This could lead to an out-of-bounds read. An attacker could leverage this vulnerability to potentially execute arbitrary code in the	N/A	A-HOR-CSCA-280623/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-27916**		
Use After Free	06-Jun-2023	7.8		N/A	A-HOR-CSCA-280623/176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The affected application lacks proper validation of user-supplied data when parsing project files (e.g., CSP). This could lead to a use-after-free vulnerability. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28653		
Stack-based Buffer Overflow	06-Jun-2023	7.8	The affected application lacks proper validation of user-supplied data when parsing project files (e.g., CSP). This could lead to a stack-based buffer overflow. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29503**	N/A	A-HOR-CSCA-280623/177
Access of Uninitialized Pointer	06-Jun-2023	7.8		N/A	A-HOR-CSCA-280623/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The affected product does not properly validate user-supplied data. If a user opens a maliciously formed CSP file, then an attacker could execute arbitrary code within the current process by accessing an uninitialized pointer.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31244		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Jun-2023	7.8		N/A	A-HOR-CSCA-280623/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The affected application lacks proper validation of user-supplied data when parsing project files (e.g., HMI). This could lead to an out-of-bounds read. An attacker could leverage this vulnerability to potentially execute arbitrary code in the context of the current process.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31278		
Out-of-bounds Write	06-Jun-2023	7.8	The affected application lacks proper validation of	N/A	A-HOR-CSCA-280623/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user-supplied data when parsing project files (e.g., HMI). This could lead to an out-of-bounds write at CScape_EnvisionRV+0x2e374b. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-32203**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.8	The affected application lacks proper validation of user-supplied data when parsing project files (e.g., CSP). This could lead to an out-of-bounds read in the FontManager. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-32281**	N/A	A-HOR-CSCA-280623/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.8	The affected application lacks proper validation of user-supplied data when parsing project files (e.g.., CSP). This could lead to an out-of-bounds read in IO_CFG. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process.	N/A	A-HOR-CSCA-280623/182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32289		
Out-of-bounds Write	06-Jun-2023	7.8	The affected application lacks proper validation of user-supplied data when parsing project files (e.g., HMI). This could lead to an out-of-bounds write at CScape_EnvisionRV+0x2e3c04. An attacker	N/A	A-HOR-CSCA-280623/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could leverage this vulnerability to potentially execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-32539**		
Out-of-bounds Read	06-Jun-2023	7.8		N/A	A-HOR-CSCA-280623/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The affected application lacks proper validation of user-supplied data when parsing project files (e.g., CSP). This could lead to an out-of-bounds read in Cscape!CANPortMigration. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32545		
Product: cscape_envisionrv					
Affected Version(s): 4.70					
Out-of-bounds Read	06-Jun-2023	7.8	The affected application lacks proper validation of user-supplied data when parsing font files (e.g., FNT). This could lead to an out-of-bounds read. An attacker could leverage this vulnerability to potentially execute arbitrary code in the context of the current process.	N/A	A-HOR-CSCA-280623/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27916		
Use After Free	06-Jun-2023	7.8		N/A	A-HOR-CSCA-280623/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The affected application lacks proper validation of user-supplied data when parsing project files (e.g., CSP). This could lead to a use-after-free vulnerability. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-28653**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	06-Jun-2023	7.8	The affected application lacks proper validation of user-supplied data when parsing project files (e.g., CSP). This could lead to a stack-based buffer overflow. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29503**	N/A	A-HOR-CSCA-280623/187
Access of Uninitialized Pointer	06-Jun-2023	7.8		N/A	A-HOR-CSCA-280623/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The affected product does not properly validate user-supplied data. If a user opens a maliciously formed CSP file, then an attacker could execute arbitrary code within the current process by accessing an uninitialized pointer.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31244		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Jun-2023	7.8		N/A	A-HOR-CSCA-280623/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The affected application lacks proper validation of user-supplied data when parsing project files (e.g., HMI). This could lead to an out-of-bounds read. An attacker could leverage this vulnerability to potentially execute arbitrary code in the context of the current process.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31278		
Out-of-bounds Write	06-Jun-2023	7.8	The affected application lacks proper validation of user-supplied data when parsing project	N/A	A-HOR-CSCA-280623/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files (e.g., HMI). This could lead to an out-of-bounds write at CScape_EnvisionRV+0x2e374b. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-32203**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.8	The affected application lacks proper validation of user-supplied data when parsing project files (e.g., CSP). This could lead to an out-of-bounds read in the FontManager. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-32281**	N/A	A-HOR-CSCA-280623/191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.8	The affected application lacks proper validation of user-supplied data when parsing project files (e.g.., CSP). This could lead to an out-of-bounds read in IO_CFG. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process.	N/A	A-HOR-CSCA-280623/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32289		
Out-of-bounds Write	06-Jun-2023	7.8	The affected application lacks proper validation of user-supplied data when parsing project files (e.g., HMI). This could lead to an out-of-bounds write at CScape_EnvisionRV+0x2e3c04. An attacker	N/A	A-HOR-CSCA-280623/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could leverage this vulnerability to potentially execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-32539**		
Out-of-bounds Read	06-Jun-2023	7.8		N/A	A-HOR-CSCA-280623/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The affected application lacks proper validation of user-supplied data when parsing project files (e.g., CSP). This could lead to an out-of-bounds read in Cscape!CANPortMigration. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32545		
Vendor: i13websolution					
Product: photo_gallery_slideshow_\&_masonry_tiled_gallery					
Affected Version(s): * Up to (including) 1.0.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	6.1	The Photo Gallery Slideshow & Masonry Tiled Gallery plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the search_term parameter in versions up to, and including, 1.0.13 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2023-2402**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2808029%40wp-responsive-photo-gallery%2Ftags%2F1.0.13&new=2905480%40wp-responsive-photo-gallery%2Ftags%2F1.0.14	A-I13-PHOT-280623/195
Product: team_circle_image_slider_with_lightbox					
Affected Version(s): * Up to (including) 1.0.17					
Improper Neutralization of Input During Web Page	09-Jun-2023	6.1	The Team Circle Image Slider With Lightbox plugin for WordPress is vulnerable to Reflected Cross-Site	https://plugins.trac.wordpress.org/changeset?old_path=%2Fcircle-image-slider-	A-I13-TEAM-280623/196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Scripting via the 'search_term' parameter in versions up to, and including, 1.0.17 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2023-2604**	with-lightbox%2Ftags%2F1.0.17&old=2910236&new_path=%2Fcircle-image-slider-with-lightbox%2Ftags%2F1.0.18&new=2910236&sfp_email=&sfph_mail=	
Product: wordpress_vertical_image_slider					
Affected Version(s): * Up to (excluding) 1.2.17					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	6.1	The wordpress vertical image slider plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'search_term' parameter in versions up to, and including, 1.2.16 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2824902%40wp-vertical-image-slider%2Ftags%2F1.2.16&new=2902084%40wp-vertical-image-slider%2Ftags%2F1.2.17	A-I13-WORD-280623/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such as clicking on a link. **CVE ID : CVE-2023-2289**		
Product: wp_responsive_tabs					
Affected Version(s): * Up to (excluding) 1.1.16					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	6.1	The WP Responsive Tabs horizontal vertical and accordion Tabs plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the search_term parameter in versions up to, and including, 1.1.15 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2023-2184**	N/A	A-I13-WP_R-280623/198
Vendor: IBM					
Product: aspera_cargo					
Affected Version(s): * Up to (excluding) 4.2.6					
Improper Restriction of Operations within the	05-Jun-2023	7.8	IBM Aspera Connect 4.2.5 and IBM Aspera Cargo 4.2.5 is vulnerable to a buffer overflow, caused by	https://exchange.xforce.ibmcloud.com/vulnerabilities/248625,	A-IBM-ASPE-280623/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			improper bounds checking. An attacker could overflow a buffer and execute arbitrary code on the system. IBM X-Force ID: 248625. **CVE ID : CVE-2023-27285**	https://www.ibm.com/support/pages/node/7001053	
Insufficiently Protected Credentials	05-Jun-2023	7.5	IBM Aspera Connect 4.2.5 and IBM Aspera Cargo 4.2.5 transmits authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval. IBM X-Force ID: 244107. **CVE ID : CVE-2023-22862**	https://www.ibm.com/support/pages/node/7001053, https://exchange.xforce.ibmcloud.com/vulnerabilities/244107	A-IBM-ASPE-280623/200
Product: aspera_connect					
Affected Version(s): * Up to (excluding) 4.2.6					
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-Jun-2023	7.8	IBM Aspera Connect 4.2.5 and IBM Aspera Cargo 4.2.5 is vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow a buffer and execute arbitrary code on the system. IBM X-Force ID: 248625. **CVE ID : CVE-2023-27285**	https://exchange.xforce.ibmcloud.com/vulnerabilities/248625, https://www.ibm.com/support/pages/node/7001053	A-IBM-ASPE-280623/201
Insufficiently	05-Jun-2023	7.5	IBM Aspera Connect 4.2.5 and IBM Aspera Cargo 4.2.5 transmits	https://www.ibm.com/support/pages/n	A-IBM-ASPE-280623/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval. IBM X-Force ID: 244107. **CVE ID : CVE-2023-22862**	ode/7001053, https://exchange.xforce.ibmcloud.com/vulnerabilities/244107	
Product: cics_tx					
Affected Version(s): 10.1					
N/A	07-Jun-2023	6.5	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 could allow a privileged user to obtain highly sensitive information by enabling debug mode. IBM X-Force ID: 257104. **CVE ID : CVE-2023-33848**	https://www.ibm.com/support/pages/node/7001683, https://exchange.xforce.ibmcloud.com/vulnerabilities/257104, https://www.ibm.com/support/pages/node/7001681, https://www.ibm.com/support/pages/node/7001647	A-IBM-CICS-280623/203
Missing Encryption of Sensitive Data	07-Jun-2023	3.7	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 could transmit sensitive information in query parameters that could be intercepted using man in the middle techniques. IBM X-Force ID: 257105.	https://www.ibm.com/support/pages/node/7001695, https://exchange.xforce.ibmcloud.com/vulnerabilities/257105, https://www.ibm.com/support/pages/node/7001697,	A-IBM-CICS-280623/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33849	https://www.ibm.com/support/pages/node/7001687	
Affected Version(s): 11.1					
N/A	07-Jun-2023	6.5	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 could allow a privileged user to obtain highly sensitive information by enabling debug mode. IBM X-Force ID: 257104. **CVE ID : CVE-2023-33848**	https://www.ibm.com/support/pages/node/7001683, https://exchange.xforce.ibmcloud.com/vulnerabilities/257104, https://www.ibm.com/support/pages/node/7001681, https://www.ibm.com/support/pages/node/7001647	A-IBM-CICS-280623/205
Missing Encryption of Sensitive Data	07-Jun-2023	3.7	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 could transmit sensitive information in query parameters that could be intercepted using man in the middle techniques. IBM X-Force ID: 257105. **CVE ID : CVE-2023-33849**	https://www.ibm.com/support/pages/node/7001695, https://exchange.xforce.ibmcloud.com/vulnerabilities/257105, https://www.ibm.com/support/pages/node/7001697, https://www.ibm.com/support/pages/node/7001687	A-IBM-CICS-280623/206
Product: maximo_application_suite					
Affected Version(s): 8.8.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	05-Jun-2023	5.9	IBM Maximo Application Suite - Manage Component 8.8.0 and 8.9.0 transmits sensitive information in cleartext that could be intercepted by an attacker using man in the middle techniques. IBM X-Force ID: 249208. **CVE ID : CVE-2023-27861**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249208, https://www.ibm.com/support/pages/node/6999917	A-IBM-MAXI-280623/207
N/A	05-Jun-2023	5.3	IBM Maximo Asset Management 7.6.1.2, 7.6.1.3 and IBM Maximo Application Suite 8.8.0 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 255074. **CVE ID : CVE-2023-32334**	https://exchange.xforce.ibmcloud.com/vulnerabilities/255074, https://www.ibm.com/support/pages/node/6999747, https://www.ibm.com/support/pages/node/6999721	A-IBM-MAXI-280623/208
Affected Version(s): 8.9.0					
Cleartext Transmission of Sensitive Information	05-Jun-2023	5.9	IBM Maximo Application Suite - Manage Component 8.8.0 and 8.9.0 transmits sensitive information in cleartext that could be intercepted by an attacker using man in	https://exchange.xforce.ibmcloud.com/vulnerabilities/249208, https://www.ibm.com/support/pages/node/6999917	A-IBM-MAXI-280623/209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the middle techniques. IBM X-Force ID: 249208. **CVE ID : CVE-2023-27861**		
Product: maximo_asset_management					
Affected Version(s): 7.6.1.2					
N/A	05-Jun-2023	5.3	IBM Maximo Asset Management 7.6.1.2, 7.6.1.3 and IBM Maximo Application Suite 8.8.0 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 255074. **CVE ID : CVE-2023-32334**	https://exchange.xforce.ibmcloud.com/vulnerabilities/255074, https://www.ibm.com/support/pages/node/6999747, https://www.ibm.com/support/pages/node/6999721	A-IBM-MAXI-280623/210
Affected Version(s): 7.6.1.3					
N/A	05-Jun-2023	5.3	IBM Maximo Asset Management 7.6.1.2, 7.6.1.3 and IBM Maximo Application Suite 8.8.0 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history.	https://exchange.xforce.ibmcloud.com/vulnerabilities/255074, https://www.ibm.com/support/pages/node/6999747, https://www.ibm.com/support/pages/node/6999721	A-IBM-MAXI-280623/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 255074. **CVE ID : CVE-2023-32334**		
Product: security_guardium					
Affected Version(s): 11.5					
Insufficient Session Expiration	05-Jun-2023	8.8	IBM Security Guardium 11.5 could allow a user to take over another user's session due to insufficient session expiration. IBM X-Force ID: 243657. **CVE ID : CVE-2023-0041**	https://www.ibm.com/support/pages/node/7000021, https://exchange.xforce.ibmcloud.com/vulnerabilities/243657	A-IBM-SECU-280623/212
Product: sterling_partner_engagement_manager					
Affected Version(s): From (including) 6.1.2 Up to (excluding) 6.1.2.8					
N/A	08-Jun-2023	9.6	IBM Sterling Partner Engagement Manager 6.1, 6.2, and 6.2.1 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 245891. **CVE ID : CVE-2023-23482**	https://exchange.xforce.ibmcloud.com/vulnerabilities/245891, https://www.ibm.com/support/pages/node/7001569	A-IBM-STER-280623/213
Improper Neutralization of	08-Jun-2023	5.4	IBM Sterling Partner Engagement Manager 6.1, 6.2, and 6.2.1 is	https://www.ibm.com/support/pages/n	A-IBM-STER-280623/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 245885. **CVE ID : CVE-2023-23480**	ode/7001563, https://exchange.xforce.ibmcloud.com/vulnerabilities/245885	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jun-2023	5.4	IBM Sterling Partner Engagement Manager 6.1, 6.2, and 6.2.1 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 245889. **CVE ID : CVE-2023-23481**	https://www.ibm.com/support/pages/node/7001561, https://exchange.xforce.ibmcloud.com/vulnerabilities/245889	A-IBM-STER-280623/215
Affected Version(s): From (including) 6.2.0 Up to (excluding) 6.2.0.6					
N/A	08-Jun-2023	9.6	IBM Sterling Partner Engagement Manager 6.1, 6.2, and 6.2.1 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a	https://exchange.xforce.ibmcloud.com/vulnerabilities/245891, https://www.ibm.com/sup	A-IBM-STER-280623/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 245891. **CVE ID : CVE-2023-23482**	port/pages/node/7001569	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jun-2023	5.4	IBM Sterling Partner Engagement Manager 6.1, 6.2, and 6.2.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 245885. **CVE ID : CVE-2023-23480**	https://www.ibm.com/support/pages/node/7001563, https://exchange.xforce.ibmcloud.com/vulnerabilities/245885	A-IBM-STER-280623/217
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jun-2023	5.4	IBM Sterling Partner Engagement Manager 6.1, 6.2, and 6.2.1 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure	https://www.ibm.com/support/pages/node/7001561, https://exchange.xforce.ibmcloud.com/vulnerabilities/245889	A-IBM-STER-280623/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			within a trusted session. IBM X-Force ID: 245889. **CVE ID : CVE-2023-23481**		
Affected Version(s): From (including) 6.2.1 Up to (excluding) 6.2.1.3					
N/A	08-Jun-2023	9.6	IBM Sterling Partner Engagement Manager 6.1, 6.2, and 6.2.1 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 245891. **CVE ID : CVE-2023-23482**	https://exchange.xforce.ibmcloud.com/vulnerabilities/245891, https://www.ibm.com/support/pages/node/7001569	A-IBM-STER-280623/219
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jun-2023	5.4	IBM Sterling Partner Engagement Manager 6.1, 6.2, and 6.2.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 245885.	https://www.ibm.com/support/pages/node/7001563, https://exchange.xforce.ibmcloud.com/vulnerabilities/245885	A-IBM-STER-280623/220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23480		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jun-2023	5.4	IBM Sterling Partner Engagement Manager 6.1, 6.2, and 6.2.1 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 245889. **CVE ID : CVE-2023-23481**	https://www.ibm.com/support/pages/node/7001561, https://exchange.xforce.ibmcloud.com/vulnerabilities/245889	A-IBM-STER-280623/221
Product: txseries_for_multiplatforms					
Affected Version(s): 8.1					
N/A	07-Jun-2023	6.5	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 could allow a privileged user to obtain highly sensitive information by enabling debug mode. IBM X-Force ID: 257104. **CVE ID : CVE-2023-33848**	https://www.ibm.com/support/pages/node/7001683, https://exchange.xforce.ibmcloud.com/vulnerabilities/257104, https://www.ibm.com/support/pages/node/7001681, https://www.ibm.com/support/pages/node/7001647	A-IBM-TXSE-280623/222
Missing Encryption	07-Jun-2023	3.7	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX	https://www.ibm.com/support/pages/n	A-IBM-TXSE-280623/223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			Standard, 11.1, CICS TX Advanced 10.1, and 11.1 could transmit sensitive information in query parameters that could be intercepted using man in the middle techniques. IBM X-Force ID: 257105. **CVE ID : CVE-2023-33849**	ode/7001695, https://exchange.xforce.ibmcloud.com/vulnerabilities/257105, https://www.ibm.com/support/pages/node/7001697, https://www.ibm.com/support/pages/node/7001687	
Affected Version(s): 8.2					
N/A	07-Jun-2023	6.5	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 could allow a privileged user to obtain highly sensitive information by enabling debug mode. IBM X-Force ID: 257104. **CVE ID : CVE-2023-33848**	https://www.ibm.com/support/pages/node/7001683, https://exchange.xforce.ibmcloud.com/vulnerabilities/257104, https://www.ibm.com/support/pages/node/7001681, https://www.ibm.com/support/pages/node/7001647	A-IBM-TXSE-280623/224
Missing Encryption of Sensitive Data	07-Jun-2023	3.7	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 could transmit sensitive information in query parameters that could be intercepted using man in the middle	https://www.ibm.com/support/pages/node/7001695, https://exchange.xforce.ibmcloud.com/vulnerabilities/257105, https://www.ibm.com/sup	A-IBM-TXSE-280623/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			techniques. IBM X-Force ID: 257105. **CVE ID : CVE-2023-33849**	port/pages/node/7001697, https://www.ibm.com/support/pages/node/7001687	
Affected Version(s): 9.1					
N/A	07-Jun-2023	6.5	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 could allow a privileged user to obtain highly sensitive information by enabling debug mode. IBM X-Force ID: 257104. **CVE ID : CVE-2023-33848**	https://www.ibm.com/support/pages/node/7001683, https://exchange.xforce.ibmcloud.com/vulnerabilities/257104, https://www.ibm.com/support/pages/node/7001681, https://www.ibm.com/support/pages/node/7001647	A-IBM-TXSE-280623/226
Missing Encryption of Sensitive Data	07-Jun-2023	3.7	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 could transmit sensitive information in query parameters that could be intercepted using man in the middle techniques. IBM X-Force ID: 257105. **CVE ID : CVE-2023-33849**	https://www.ibm.com/support/pages/node/7001695, https://exchange.xforce.ibmcloud.com/vulnerabilities/257105, https://www.ibm.com/support/pages/node/7001697, https://www.ibm.com/support/pages/node/7001687	A-IBM-TXSE-280623/227
Vendor: ibos					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ibos					
Affected Version(s): 4.5.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jun-2023	9.8	A vulnerability, which was classified as critical, has been found in IBOS 4.5.5. Affected by this issue is the function actionDel of the file ?r=dashboard/approval/del. The manipulation of the argument id leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-230690 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-2023-3100**	N/A	A-IBO-IBOS-280623/228
Vendor: Imagemagick					
Product: imagemagick					
Affected Version(s): * Up to (excluding) 7.1.1-9					
Out-of-bounds Write	06-Jun-2023	5.5	A heap-based buffer overflow vulnerability was found in the ImageMagick package that can lead to the application crashing. **CVE ID : CVE-2023-2157**	https://bugzilla.redhat.com/show_bug.cgi?id=2208537	A-IMA-IMAG-280623/229
Vendor: imperial_cms_project					
Product: imperial_cms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 7.5					
N/A	07-Jun-2023	9.1	Imperial CMS v7.5 was discovered to contain an arbitrary file deletion vulnerability via the DelspReFile function in /sp/ListSp.php. This vulnerability is exploited by attackers via a crafted POST request. **CVE ID : CVE-2023-33604**	N/A	A-IMP-IMPE-280623/230
Vendor: iniparser_project					
Product: iniparser					
Affected Version(s): 4.1					
NULL Pointer Dereference	01-Jun-2023	5.5	iniparser v4.1 is vulnerable to NULL Pointer Dereference in function iniparser_getlongint which misses check NULL for function iniparser_getstring's return. **CVE ID : CVE-2023-33461**	https://github.com/ndevilla/iniparser/issues/144	A-INI-INIP-280623/231
Vendor: inpiazza					
Product: cloud_wifi					
Affected Version(s): * Up to (excluding) 4.2.17					
Improper Restriction of Excessive Authentication Attempts	01-Jun-2023	6.5	The captive portal in Inpiazza Cloud WiFi versions prior to v4.2.17 does not enforce limits on the number of attempts for password recovery, allowing attackers to brute	N/A	A-INP-CLOU-280623/232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			force valid user accounts to gain access to login credentials. **CVE ID : CVE-2023-33754**		
Vendor: iptanus					
Product: wordpress_file_upload					
Affected Version(s): * Up to (including) 4.19.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	5.5	The WordPress File Upload and WordPress File Upload Pro plugins for WordPress are vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 4.19.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-2767**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2915978%40wp-file-upload%2Ftrunk&old=2909107%40wp-file-upload%2Ftrunk&sfp_email=&sfph_mail=#file2	A-IPT-WORD-280623/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Jun-2023	4.9	The WordPress File Upload and WordPress File Upload Pro plugins for WordPress are vulnerable to Path Traversal in versions up to, and including, 4.19.1 via the vulnerable parameter wfu_newpath. This allows administrator-level attackers to move files uploaded with the plugin (located in wp-content/uploads by default) outside of the web root. **CVE ID : CVE-2023-2688**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2915978%40wp-file-upload%2Ftrunk&old=2909107%40wp-file-upload%2Ftrunk&sfp_email=&sfph_mail=#file2	A-IPT-WORD-280623/234
Product: wordpress_file_upload_pro					
Affected Version(s): * Up to (including) 4.19.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	5.5	The WordPress File Upload and WordPress File Upload Pro plugins for WordPress are vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 4.19.1 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	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2915978%40wp-file-upload%2Ftrunk&old=2909107%40wp-file-upload%2Ftrunk&sfp_email=&sfph_mail=#file2	A-IPT-WORD-280623/235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-2767**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Jun-2023	4.9	The WordPress File Upload and WordPress File Upload Pro plugins for WordPress are vulnerable to Path Traversal in versions up to, and including, 4.19.1 via the vulnerable parameter wfu_newpath. This allows administrator-level attackers to move files uploaded with the plugin (located in wp-content/uploads by default) outside of the web root. **CVE ID : CVE-2023-2688**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2915978%40wp-file-upload%2Ftrunk&old=2909107%40wp-file-upload%2Ftrunk&sfp_email=&sfph_mail=#file2	A-IPT-WORD-280623/236
Vendor: ip_metaboxes_project					
Product: ip_metaboxes					
Affected Version(s): * Up to (including) 2.1.1					
Improper Neutralization of Input During Web Page Generation	12-Jun-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Phan Chuong IP Metaboxes plugin <= 2.1.1.	N/A	A-IP_-IP_M-280623/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-30753**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jun-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Phan Chuong IP Metaboxes plugin <= 2.1.1 versions. **CVE ID : CVE-2023-30745**	N/A	A-IP_-IP_M-280623/238
Vendor: itemprop_wp_for_serp\/seo_rich_snippets_project					
Product: itemprop_wp_for_serp\/seo_rich_snippets					
Affected Version(s): * Up to (including) 3.5.201706131					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jun-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Rolands Umbrovskis itemprop WP for SERP/SEO Rich snippets plugin <= 3.5.201706131 versions. **CVE ID : CVE-2023-23819**	N/A	A-ITE-ITEM-280623/239
Vendor: itpison					
Product: omicard_edm					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	02-Jun-2023	6.8	OMICARD EDM backend system's file uploading function does not restrict upload of file with dangerous type. A local area network attacker with administrator privileges can exploit this vulnerability to upload and run	N/A	A-ITP-OMIC-280623/240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary executable files to perform arbitrary system commands or disrupt service. **CVE ID : CVE-2023-28700**		
Vendor: iuok					
Product: yfcmf-tp6					
Affected Version(s): * Up to (including) 3.0.4					
Path Traversal: '../filedir'	02-Jun-2023	9.8	A vulnerability was found in YFCMF up to 3.0.4. It has been declared as problematic. This vulnerability affects unknown code of the file index.php. The manipulation leads to path traversal: '../filedir'. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-230542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3056**	N/A	A-IUO-YFCM-280623/241
Path Traversal: '../filedir'	02-Jun-2023	9.8	A vulnerability was found in YFCMF up to 3.0.4. It has been rated as problematic. This issue affects some unknown processing of the file app/admin/controller/Ajax.php. The manipulation of the argument controllername leads	N/A	A-IUO-YFCM-280623/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to path traversal: '../filedir'. 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-230543. **CVE ID : CVE-2023-3057**		
Vendor: janino_project					
Product: janino					
Affected Version(s): * Up to (including) 3.1.9					
Out-of-bounds Write	01-Jun-2023	5.5	janino 3.1.9 and earlier are subject to denial of service (DOS) attacks when using the expression evaluator.guess parameter name method. If the parser runs on user-supplied input, an attacker could supply content that causes the parser to crash due to a stack overflow. **CVE ID : CVE-2023-33546**	N/A	A-JAN-JANI-280623/243
Vendor: jeecg_p3_biz_chat_project					
Product: jeecg_p3_biz_chat					
Affected Version(s): 1.0.5					
Exposure of Resource to Wrong Sphere	07-Jun-2023	7.5	Jeecg P3 Biz Chat 1.0.5 allows remote attackers to read arbitrary files through specific parameters.	N/A	A-JEE-JEEC-280623/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33510		
Vendor: Jetbrains					
Product: ktor					
Affected Version(s): * Up to (excluding) 2.3.1					
Generation of Error Message Containing Sensitive Information	01-Jun-2023	3.3	In JetBrains Ktor before 2.3.1 headers containing authentication data could be added to the exception's message **CVE ID : CVE-2023-34339**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-KTOR-280623/245
Vendor: jmsthemelayout_project					
Product: jmsthemelayout					
Affected Version(s): 2.5.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jun-2023	9.8	PrestaShop jmsthemelayout 2.5.5 is vulnerable to SQL Injection via ajax_jmsvermegamenu.php. **CVE ID : CVE-2023-29629**	N/A	A-JMS-JMST-280623/246
Vendor: joommasters					
Product: jmspagebuilder					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jun-2023	9.8	PrestaShop jmspagebuilder 3.x is vulnerable to SQL Injection via ajax_jmspagebuilder.php. **CVE ID : CVE-2023-29632**	https://friends-of-presta.github.io/security-advisories/modules/2023/03/13/jmspagebuilder.html	A-JOO-JMSP-280623/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: jms_drop_mega_menu					
Affected Version(s): 1.0.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jun-2023	9.8	PrestaShop jmsmegamenu 1.1.x and 2.0.x is vulnerable to SQL Injection via ajax_jmsmegamenu.php. **CVE ID : CVE-2023-29630**	N/A	A-JOO-JMS_-280623/248
Affected Version(s): 2.0.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jun-2023	9.8	PrestaShop jmsmegamenu 1.1.x and 2.0.x is vulnerable to SQL Injection via ajax_jmsmegamenu.php. **CVE ID : CVE-2023-29630**	N/A	A-JOO-JMS_-280623/249
Product: jms_slider					
Affected Version(s): 1.6.0					
Unrestricted Upload of File with Dangerous Type	05-Jun-2023	9.8	PrestaShop jmsslider 1.6.0 is vulnerable to Incorrect Access Control via ajax_jmsslider.php. **CVE ID : CVE-2023-29631**	N/A	A-JOO-JMS_-280623/250
Vendor: Kanboard					
Product: kanboard					
Affected Version(s): * Up to (excluding) 1.2.30					
Authorization Bypass Through User-	05-Jun-2023	6.5	Kanboard is open source project management software that focuses on the Kanban methodology.	https://github.com/kanboard/kanboard/commit/437b141fa2267df3	A-KAN-KANB-280623/251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Key			Versions prior to 1.2.30 are subject to an Insecure direct object reference (IDOR) vulnerability present in the application's URL parameter. This vulnerability enables any user to read files uploaded by any other user, regardless of their privileges or restrictions. By Changing the file_id any user can render all the files where MimeType is image uploaded under **/files** directory regard less of uploaded by any user. This vulnerability poses a significant impact and severity to the application's security. By manipulating the URL parameter, an attacker can access sensitive files that should only be available to authorized users. This includes confidential documents or any other type of file stored within the application. The ability to read these files can lead to various detrimental consequences, such as unauthorized disclosure of sensitive	6976814e704517f30d2424bd	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information, privacy breaches, intellectual property theft, or exposure of trade secrets. Additionally, it could result in legal and regulatory implications, reputation damage, financial losses, and potential compromise of user trust. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-33956**		
Missing Authorization	05-Jun-2023	6.5	Kanboard is open source project management software that focuses on the Kanban methodology. A vulnerability related to a `missing access control` was found, which allows a User with the lowest privileges to leak all the tasks and projects titles within the software, even if they are not invited or it's a personal project. This could also lead to private/critical information being leaked if such information is in the title. This issue has been addressed in	https://github.com/kanboard/kanboard/commit/b501ef44bc28ee9cf603a4fa446ee121d66f652f	A-KAN-KANB-280623/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 1.2.30. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-33970**		
Missing Authorization	05-Jun-2023	5.4	Kanboard is open source project management software that focuses on the Kanban methodology. Versions prior to 1.2.30 are subject to a missing access control vulnerability that allows a user with low privileges to create or transfer tasks to any project within the software, even if they have not been invited or the project is personal. The vulnerable features are `Duplicate to project` and `Move to project`, which both utilize the `checkDestinationProjectValues()` function to check his values. This issue has been addressed in version 1.2.30. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-33968**	https://github.com/kanboard/kanboard/commit/c20be8f5fa26e54005a90c645e80b11481a65053	A-KAN-KANB-280623/253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2023	5.4	Kanboard is open source project management software that focuses on the Kanban methodology. A stored Cross site scripting (XSS) allows an attacker to execute arbitrary Javascript and any user who views the task containing the malicious code will be exposed to the XSS attack. Note: The default CSP header configuration blocks this javascript attack. This issue has been addressed in version 1.2.30. Users are advised to upgrade. Users unable to upgrade should ensure that they have a restrictive CSP header config. **CVE ID : CVE-2023-33969**	https://github.com/kanboard/kanboard/commit/05f1d23d821152cd61536d3b09e522c0f7573e3c	A-KAN-KANB-280623/254
Vendor: Kibokolabs					
Product: hostel					
Affected Version(s): * Up to (including) 1.1.5					
Improper Neutralization of Input During Web Page Generation	05-Jun-2023	4.8	The Hostel WordPress plugin before 1.1.5.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-	N/A	A-KIB-HOST-280623/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID : CVE-2023-0545**		
Vendor: kiwitcms					
Product: kiwi_tcms					
Affected Version(s): * Up to (including) 12.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-2023	5.4	Kiwi TCMS is an open source test management system for both manual and automated testing. Kiwi TCMS allows users to upload attachments to test plans, test cases, etc. Earlier versions of Kiwi TCMS had introduced upload validators in order to prevent potentially dangerous files from being uploaded and Content-Security-Policy definition to prevent cross-site-scripting attacks. The upload validation checks were not 100% robust which left the possibility to circumvent them and upload a potentially dangerous file which allows execution of arbitrary JavaScript in the browser.	https://github.com/kiwitcms/Kiwi/commit/d789f4b51025de4f8c747c037d02e1b0da80b034, https://github.com/kiwitcms/Kiwi/security/advisories/GHSA-2fqm-m4r2-fh98, https://huntr.dev/bounties/6aea9a26-e29a-467b-aa5a-f767f0c2ec96/	A-KIW-KIWI-280623/256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Additionally we've discovered that Nginx's `proxy_pass` directive will strip some headers negating protections built into Kiwi TCMS when served behind a reverse proxy. This issue has been addressed in version 12.4. Users are advised to upgrade. Users unable to upgrade who are serving Kiwi TCMS behind a reverse proxy should make sure that additional header values are still passed to the client browser. If they aren't redefining them inside the proxy configuration. **CVE ID : CVE-2023-33977**		
Vendor: knime					
Product: business_hub					
Affected Version(s): * Up to (excluding) 1.4.0					
N/A	07-Jun-2023	5.3	The Web Frontend of KNIME Business Hub before 1.4.0 allows an unauthenticated remote attacker to access internals about the application such as versions, host names, or IP addresses. No personal information or application data was exposed.	https://www.knime.com/security/advisories#CVE-2023-2541	A-KNI-BUSI-280623/257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2541		
Vendor: kylinos					
Product: kylin-software-properties					
Affected Version(s): * Up to (excluding) 0.0.1-130					
N/A	05-Jun-2023	7.8	A vulnerability was found in KylinSoft kylin-software-properties on KylinOS. It has been declared as critical. This vulnerability affects the function changedSource. The manipulation leads to improper access controls. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. Upgrading to version 0.0.1-130 is able to address this issue. It is recommended to upgrade the affected component. VDB-230686 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	A-KYL-KYLI-280623/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3096		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jun-2023	7.8	A vulnerability was found in KylinSoft kylin-software-properties on KylinOS. It has been rated as critical. This issue affects the function setMainSource. The manipulation leads to os command injection. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. Upgrading to version 0.0.1-130 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-230687. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3097**	N/A	A-KYL-KYLI-280623/259
Vendor: libcap_project					
Product: libcap					
Affected Version(s): 2.66					
Missing Release of Memory after	06-Jun-2023	3.3	A vulnerability was found in the pthread_create() function in libcap. This issue may allow a	N/A	A-LIB-LIBC-280623/260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			malicious actor to use cause __real_pthread_create( ) to return an error, which can exhaust the process memory. **CVE ID : CVE-2023-2602**		
Vendor: life_insurance_management_system_project					
Product: life_insurance_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jun-2023	6.1	A vulnerability was found in SourceCodester Life Insurance Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file insertNominee.php of the component POST Parameter Handler. The manipulation of the argument nominee_id leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-231109 was assigned to this vulnerability. **CVE ID : CVE-2023-3165**	N/A	A-LIF-LIFE-280623/261
Vendor: Linuxfoundation					
Product: iot-yocto					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 22.2					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-IOT--280623/262
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-IOT--280623/263
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-IOT--280623/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-IOT--280623/265
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-IOT--280623/266
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a 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/June-2023	A-LIN-IOT--280623/267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-IOT--280623/268
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-IOT--280623/269
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation	https://corp.mediatek.com/product-security-	A-LIN-IOT--280623/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	bulletin/June-2023	
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519142. **CVE ID : CVE-2023-20743**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-IOT--280623/271
Use After Free	06-Jun-2023	6.7	In vcu, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519200. **CVE ID : CVE-2023-20744**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-IOT--280623/272
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds	https://corp.mediatek.com	A-LIN-IOT--280623/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07560694. **CVE ID : CVE-2023-20745**	/product-security-bulletin/June-2023	
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-IOT--280623/274
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189.	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-IOT--280623/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20736		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-IOT--280623/276
Product: yocto					
Affected Version(s): 3.1					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/277
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573575. **CVE ID : CVE-2023-20729**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/279
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573552. **CVE ID : CVE-2023-20730**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/280
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-	A-LIN-YOCT-280623/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	bulletin/June-2023	
Affected Version(s): 3.3					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/282
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573575. **CVE ID : CVE-2023-20729**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/284
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573552. **CVE ID : CVE-2023-20730**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/285
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**		
Affected Version(s): 4.0					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/287
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/288
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/290
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/291
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This	https://corp.mediatek.com/product-security-	A-LIN-YOCT-280623/292

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: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/293
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/295
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/296
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07519142; Issue ID: ALPS07519142. **CVE ID : CVE-2023-20743**		
Use After Free	06-Jun-2023	6.7	In vcu, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519200. **CVE ID : CVE-2023-20744**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/298
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07560694. **CVE ID : CVE-2023-20745**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/299
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/301
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/302
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-	A-LIN-YOCT-280623/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573575. **CVE ID : CVE-2023-20729**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/304
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573552. **CVE ID : CVE-2023-20730**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/306
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-LIN-YOCT-280623/307
Vendor: lost_and_found_information_system_project					
Product: lost_and_found_information_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command	09-Jun-2023	8.8	A vulnerability, which was classified as critical, was found in SourceCodester Lost and Found Information System 1.0. Affected is an unknown function of the file	N/A	A-LOS-LOST-280623/308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			admin\user\manage_user.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-231150 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3176**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Jun-2023	8.8	A vulnerability has been found in SourceCodester Lost and Found Information System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file admin\inquiries\view_inquiry.php. The manipulation leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-231151. **CVE ID : CVE-2023-3177**	N/A	A-LOS-LOST-280623/309
Vendor: Mailcow					
Product: mailcow					
Affected Version(s): _dockerized Up to (including) 2023-05					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Jun-2023	8.8	mailcow is a mail server suite based on Dovecot, Postfix and other open source software, that provides a modern web UI for user/server administration. A vulnerability has been discovered in mailcow which allows an attacker to manipulate internal Dovecot variables by using specially crafted passwords during the authentication process. The issue arises from the behavior of the `passwd-verify.lua` script, which is responsible for verifying user passwords during login attempts. Upon a successful login, the script returns a response in the format of "password=<valid-password>", indicating the successful authentication. By crafting a password with additional key-value pairs appended to it, an attacker can manipulate the returned string and influence the internal behavior of Dovecot. For example, using the	https://github.com/mailcow/mailcow-dockerized/commit/f80940efdccd393bf5fccec2886795372a38c445, https://github.com/mailcow/mailcow-dockerized/security/advisories/GHSA-mhh4-qchc-pv22	A-MAI-MAIL-280623/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password "123 mail_crypt_save_version=0" would cause the `passwd-verify.lua` script to return the string "password=123 mail_crypt_save_version=0". Consequently, Dovecot will interpret this string and set the internal variables accordingly, leading to unintended consequences. This vulnerability can be exploited by an authenticated attacker who has the ability to set their own password. Successful exploitation of this vulnerability could result in unauthorized access to user accounts, bypassing security controls, or other malicious activities. This issue has been patched in version `2023-05a`. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-34108**		
Vendor: marsctf_project					
Product: marsctf					
Affected Version(s): 1.2.1					
Unrestricted Upload of File with	05-Jun-2023	9.8	MarsCTF 1.2.1 has an arbitrary file upload vulnerability in the	N/A	A-MAR-MARS-280623/311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			interface for uploading attachments in the background. **CVE ID : CVE-2023-33386**		
Vendor: marvalglobal					
Product: msm					
Affected Version(s): * Up to (including) 14.19.0.12476					
Incorrect Default Permissions	07-Jun-2023	9.8	Marval MSM through 14.19.0.12476 and 15.0 has a System account with default credentials. A remote attacker is able to login and create a valid session. This makes it possible to make backend calls to endpoints in the application. **CVE ID : CVE-2023-33282**	N/A	A-MAR-MSM-280623/312
Deserialization of Untrusted Data	07-Jun-2023	8.8	Marval MSM through 14.19.0.12476 and 15.0 has a Remote Code Execution vulnerability. A remote attacker authenticated as any user is able to execute code in context of the web server. **CVE ID : CVE-2023-33284**	N/A	A-MAR-MSM-280623/313
Inadequate Encryption Strength	07-Jun-2023	5.5	Marval MSM through 14.19.0.12476 uses a static encryption key for secrets. An attacker that gains access to encrypted	N/A	A-MAR-MSM-280623/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			secrets can decrypt them by using this key. **CVE ID : CVE-2023-33283**		
Affected Version(s): 15.0					
Incorrect Default Permissions	07-Jun-2023	9.8	Marval MSM through 14.19.0.12476 and 15.0 has a System account with default credentials. A remote attacker is able to login and create a valid session. This makes it possible to make backend calls to endpoints in the application. **CVE ID : CVE-2023-33282**	N/A	A-MAR-MSM-280623/315
Deserialization of Untrusted Data	07-Jun-2023	8.8	Marval MSM through 14.19.0.12476 and 15.0 has a Remote Code Execution vulnerability. A remote attacker authenticated as any user is able to execute code in context of the web server. **CVE ID : CVE-2023-33284**	N/A	A-MAR-MSM-280623/316
Vendor: Matrix					
Product: synapse					
Affected Version(s): * Up to (excluding) 1.85.0					
Improper Authentication	06-Jun-2023	5.4	Synapse is a Matrix protocol homeserver written in Python with the Twisted framework. In affected versions it may be	https://github.com/matrix-org/synapse/security/advisories/GHSA-	A-MAT-SYNA-280623/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible for a deactivated user to login when using uncommon configurations. This only applies if any of the following are true: 1. JSON Web Tokens are enabled for login via the `jwt_config.enabled` configuration setting. 2. The local password database is enabled via the `password_config.enabled` and `password_config.localdb_enabled` configuration settings *and* a user's password is updated via an admin API after a user is deactivated. Note that the local password database is enabled by default, but it is uncommon to set a user's password after they've been deactivated. Installations that are configured to only allow login via Single Sign-On (SSO) via CAS, SAML or OpenID Connect (OIDC); or via an external password provider (e.g. LDAP) are not affected. If not using JSON Web Tokens, ensure that deactivated users do not have a password	26c5-ppr8-f33p, https://github.com/matrix-org/synapse/pull/15624, https://github.com/matrix-org/synapse/pull/15634	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			set. This issue has been addressed in version 1.85.0. Users are advised to upgrade. **CVE ID : CVE-2023-32682**		
Server-Side Request Forgery (SSRF)	06-Jun-2023	5.4	Synapse is a Matrix protocol homeserver written in Python with the Twisted framework. A discovered oEmbed or image URL can bypass the `url_preview_url_blacklist` setting potentially allowing server side request forgery or bypassing network policies. Impact is limited to IP addresses allowed by the `url_preview_ip_range_blacklist` setting (by default this only allows public IPs) and by the limited information returned to the client: 1. For discovered oEmbed URLs, any non-JSON response or a JSON response which includes non-oEmbed information is discarded. 2. For discovered image URLs, any non-image response is discarded. Systems which have URL preview disabled	https://github.com/matrix-org/synapse/security/advisories/GHSA-98px-6486-j7qc, https://github.com/matrix-org/synapse/pull/15601	A-MAT-SYNA-280623/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(via the `url_preview_enabled` setting) or have not configured a `url_preview_url_blacklist` are not affected. This issue has been addressed in version 1.85.0. Users are advised to upgrade. User unable to upgrade may also disable URL previews. **CVE ID : CVE-2023-32683**		
Vendor: mbconnectline					
Product: mbconnect24					
Affected Version(s): * Up to (including) 2.13.3					
Authorization Bypass Through User-Controlled Key	06-Jun-2023	8.8	An Authorization Bypass vulnerability was found in MB Connect Lines mbCONNECT24, mymbCONNECT24 and Helmholz' myREX24 and myREX24.virtual version <= 2.13.3. An authenticated remote user with low privileges can change the password of any user in the same account. This allows to take over the admin user and therefore fully compromise the account. **CVE ID : CVE-2023-0985**	N/A	A-MBC-MBCO-280623/319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Jun-2023	4.3	Exposure of Sensitive Information to an unauthorized actor vulnerability in MB Connect Lines mbCONNECT24, mymbCONNECT24 and Helmholz' myREX24 and myREX24.virtual in versions <=2.13.3 allow an authorized remote attacker with low privileges to view a limited amount of another accounts contact information. **CVE ID : CVE-2023-1779**	N/A	A-MBC-MBCO-280623/320
Product: mymbconnect24					
Affected Version(s): * Up to (including) 2.13.3					
Authorization Bypass Through User-Controlled Key	06-Jun-2023	8.8	An Authorization Bypass vulnerability was found in MB Connect Lines mbCONNECT24, mymbCONNECT24 and Helmholz' myREX24 and myREX24.virtual version <= 2.13.3. An authenticated remote user with low privileges can change the password of any user in the same account. This allows to take over the admin user and therefore fully compromise the account.	N/A	A-MBC-MYMB-280623/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0985		
N/A	06-Jun-2023	4.3	Exposure of Sensitive Information to an unauthorized actor vulnerability in MB Connect Lines mbCONNECT24, mymbCONNECT24 and Helmholz' myREX24 and myREX24.virtual in versions <=2.13.3 allow an authorized remote attacker with low privileges to view a limited amount of another accounts contact information. **CVE ID : CVE-2023-1779**	N/A	A-MBC-MYMB-280623/322
Vendor: mgt-commerce					
Product: cloudpanel					
Affected Version(s): From (including) 2.0.0 Up to (including) 2.2.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jun-2023	7.8	CloudPanel v2.2.2 allows attackers to execute a path traversal. **CVE ID : CVE-2023-33747**	N/A	A-MGT-CLOU-280623/323
Vendor: Microsoft					
Product: 365_apps					
Affected Version(s): -					
N/A	05-Jun-2023	7.3	Microsoft Office Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	A-MIC-365_-280623/324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29344	bility/CVE-2023-29344	
Product: edge_chromium					
Affected Version(s): * Up to (excluding) 114.0.1823.37					
N/A	03-Jun-2023	7.5	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-33143**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33143	A-MIC-EDGE-280623/325
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2023	6.1	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29345**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29345	A-MIC-EDGE-280623/326
Product: office					
Affected Version(s): 2019					
N/A	05-Jun-2023	7.3	Microsoft Office Remote Code Execution Vulnerability **CVE ID : CVE-2023-29344**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29344	A-MIC-OFFI-280623/327
Product: office_long_term_servicing_channel					
Affected Version(s): 2021					
N/A	05-Jun-2023	7.3	Microsoft Office Remote Code Execution Vulnerability **CVE ID : CVE-2023-29344**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29344	A-MIC-OFFI-280623/328
Vendor: Microweber					
Product: microweber					
Affected Version(s): * Up to (excluding) 2.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 2.0. **CVE ID : CVE-2023-3142**	https://huntr.dev/bounties/d00686b0-f89a-4e14-98d7-b8dd3f92a6e5, https://github.com/microweber/microweber/commit/42efa981a2239d042d910069952d6276497bdcf1	A-MIC-MICR-280623/329
Vendor: minical					
Product: minical					
Affected Version(s): 1.0.0					
Improper Neutralization of Formula Elements in a CSV File	05-Jun-2023	8.8	Minical 1.0.0 and earlier contains a CSV injection vulnerability which allows an attacker to execute remote code. The vulnerability exists due to insufficient input validation on the Customer Name field in the Accounting module that is used to construct a CSV file. **CVE ID : CVE-2023-33410**	N/A	A-MIN-MINI-280623/330
Cross-Site Request Forgery (CSRF)	05-Jun-2023	6.5	Minical 1.0.0 is vulnerable to Cross Site Request Forgery (CSRF) via minical/public/application/controllers/settings/company.php.	N/A	A-MIN-MINI-280623/331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33409		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2023	5.4	Minical 1.0.0 is vulnerable to Cross Site Scripting (XSS). The vulnerability exists due to insufficient input validation in the application's user input handling in the security_helper.php file. **CVE ID : CVE-2023-33408**	N/A	A-MIN-MINI-280623/332
Vendor: miniorange					
Product: active_directory_integration_\/_ldap_integration					
Affected Version(s): * Up to (including) 4.1.4					
Cross-Site Request Forgery (CSRF)	09-Jun-2023	6.5	The Active Directory Integration plugin for WordPress is vulnerable to Cross-Site Request Forgery leading to time-based SQL Injection via the orderby and order parameters in versions up to, and including, 4.1.4 due to missing nonce verification on the get_users function and insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries	https://plugins.trac.wordpress.org/browser/ldap-login-for-intranet-sites/trunk/class-mo-ldap-user-auth-reports.php?rev=2859403#L64	A-MIN-ACTI-280623/333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into already existing queries that can be used to cause resource exhaustion via a forged request granted they can trick an administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-2599**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Jun-2023	4.9	The Active Directory Integration plugin for WordPress is vulnerable to time-based SQL Injection via the orderby and order parameters in versions up to, and including, 4.1.4 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 administrator privileges to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-2484**	https://plugins.trac.wordpress.org/browser/ldap-login-for-intranet-sites/trunk/class-mo-ldap-user-auth-reports.php?rev=2859403#L64	A-MIN-ACTI-280623/334
Vendor: mobatime					
Product: amxgt_100					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.3.20					
Improper Authentication	05-Jun-2023	9.1	Improper Authentication vulnerability in Mobatime mobile application AMXGT100 allows Authentication Bypass.This issue affects Mobatime mobile application AMXGT100 through 1.3.20. **CVE ID : CVE-2023-3065**	N/A	A-MOB-AMXG-280623/335
Authorization Bypass Through User-Controlled Key	05-Jun-2023	8.1	Incorrect Authorization vulnerability in Mobatime mobile application AMXGT100 allows a low-privileged user to impersonate anyone else, including administratorsThis issue affects Mobatime mobile application AMXGT100: through 1.3.20. **CVE ID : CVE-2023-3066**	N/A	A-MOB-AMXG-280623/336
Insecure Storage of Sensitive Information	05-Jun-2023	5.3	Anonymous user may get the list of existing users managed by the application, that could ease further attacks (see CVE-2023-3065	N/A	A-MOB-AMXG-280623/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 3066)This issue affects Mobatime mobile application AMXGT100 through 1.3.20. **CVE ID : CVE-2023-3064**		
Product: mobatime_web_application					
Affected Version(s): * Up to (including) 06.7.22					
Unrestricted Upload of File with Dangerous Type	02-Jun-2023	8.8	Unrestricted Upload of File with Dangerous Type vulnerability in Mobatime web application (Documentary proof upload modules) allows a malicious user to Upload a Web Shell to a Web Server.This issue affects Mobatime web application: through 06.7.22. **CVE ID : CVE-2023-3032**	N/A	A-MOB-MOBA-280623/338
Incorrect Authorization	02-Jun-2023	8.8	Incorrect Authorization vulnerability in Mobatime web application allows Privilege Escalation, Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Mobatime web	N/A	A-MOB-MOBA-280623/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application: through 06.7.22. **CVE ID : CVE-2023-3033**		
Vendor: motopress					
Product: getwid_-_gutenberg_blocks					
Affected Version(s): * Up to (including) 1.8.3					
Server-Side Request Forgery (SSRF)	09-Jun-2023	9.6	The Getwid – Gutenberg Blocks plugin for WordPress is vulnerable to Server Side Request Forgery via the get_remote_content REST API endpoint in versions up to, and including, 1.8.3. This can allow authenticated attackers with subscriber-level permissions or above to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. **CVE ID : CVE-2023-1895**	N/A	A-MOT-GETW-280623/340
Improper Authorization	09-Jun-2023	4.3	The Getwid – Gutenberg Blocks plugin for WordPress is vulnerable to unauthorized modification of data due to an insufficient	N/A	A-MOT-GETW-280623/341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			capability check on the get_remote_templates function in versions up to, and including, 1.8.3. This makes it possible for authenticated attackers with subscriber-level permissions or above to flush the remote template cache. Cached template information can also be accessed via this endpoint but these are not considered sensitive as they are publicly accessible from the developer's site. **CVE ID : CVE-2023-1910**		
Vendor: Mozilla					
Product: firefox					
Affected Version(s): * Up to (excluding) 109.0					
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 108 and Firefox ESR 102.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code.	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://www.mozilla.org/security/advisories/mfsa2023-03/, https://www.mozilla.org/security/advisories/mfsa2023-02/	A-MOZ-FIRE-280623/342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability affects Firefox < 109, Thunderbird < 102.7, and Firefox ESR < 102.7. **CVE ID : CVE-2023-23605**		
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 108. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 109. **CVE ID : CVE-2023-23606**	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://bugzilla.mozilla.org/buglist.cgi?bug_id=1764974%2C1798591%2C1799201%2C1800446%2C1801248%2C1802100%2C1803393%2C1804626%2C1804971%2C1807004	A-MOZ-FIRE-280623/343
Inadequate Encryption Strength	02-Jun-2023	6.5	A compromised web child process could disable web security opening restrictions, leading to a new child process being spawned within the <code>file://</code> context. Given a reliable exploit primitive, this new process could be exploited again leading to arbitrary file read. This vulnerability affects Firefox < 109.	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://bugzilla.mozilla.org/show_bug.cgi?id=1538028	A-MOZ-FIRE-280623/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23597		
N/A	02-Jun-2023	6.5	Due to the Firefox GTK wrapper code's use of text/plain for drag data and GTK treating all text/plain MIMEs containing file URLs as being dragged a website could arbitrarily read a file via a call to <code>DataTransfer.setData</code>. This vulnerability affects Firefox < 109, Thunderbird < 102.7, and Firefox ESR < 102.7. **CVE ID : CVE-2023-23598**	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://www.mozilla.org/security/advisories/mfsa2023-03/, https://www.mozilla.org/security/advisories/mfsa2023-02/, https://bugzilla.mozilla.org/show_bug.cgi?id=1800425	A-MOZ-FIRE-280623/345
Improper Encoding or Escaping of Output	02-Jun-2023	6.5	When copying a network request from the developer tools panel as a curl command the output was not being properly sanitized and could allow arbitrary commands to be hidden within. This vulnerability affects Firefox < 109, Thunderbird < 102.7, and Firefox ESR < 102.7. **CVE ID : CVE-2023-23599**	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://www.mozilla.org/security/advisories/mfsa2023-03/, https://www.mozilla.org/security/advisories/mfsa2023-02/, https://bugzilla.mozilla.org/show_bug.cgi?id=1777800	A-MOZ-FIRE-280623/346
N/A	02-Jun-2023	6.5	Per origin notification permissions were being stored in a way	https://www.mozilla.org/security/adviso	A-MOZ-FIRE-280623/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that didn't take into account what browsing context the permission was granted in. This lead to the possibility of notifications to be displayed during different browsing sessions. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 109. **CVE ID : CVE-2023-23600**	ries/mfsa2023-01/, https://bugzilla.mozilla.org/show_bug.cgi?id=1787034	
Origin Validation Error	02-Jun-2023	6.5	Navigations were being allowed when dragging a URL from a cross-origin iframe into the same tab which could lead to website spoofing attacks. This vulnerability affects Firefox < 109, Thunderbird < 102.7, and Firefox ESR < 102.7. **CVE ID : CVE-2023-23601**	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://www.mozilla.org/security/advisories/mfsa2023-03/, https://bugzilla.mozilla.org/show_bug.cgi?id=1794268, https://www.mozilla.org/security/advisories/mfsa2023-02/	A-MOZ-FIRE-280623/348
Improper Check for Unusual or Exceptiona	02-Jun-2023	6.5	A mishandled security check when creating a WebSocket in a WebWorker caused the Content Security	https://www.mozilla.org/security/advisories/mfsa2023-01/,	A-MOZ-FIRE-280623/349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			Policy connect-src header to be ignored. This could lead to connections to restricted origins from inside WebWorkers. This vulnerability affects Firefox < 109, Thunderbird < 102.7, and Firefox ESR < 102.7. **CVE ID : CVE-2023-23602**	https://www.mozilla.org/security/advisories/mfsa2023-03/, https://www.mozilla.org/security/advisories/mfsa2023-02/, https://bugzilla.mozilla.org/show_bug.cgi?id=1800890	
N/A	02-Jun-2023	6.5	Regular expressions used to filter out forbidden properties and values from style directives in calls to <code>console.log</code> weren't accounting for external URLs. Data could then be potentially exfiltrated from the browser. This vulnerability affects Firefox < 109, Thunderbird < 102.7, and Firefox ESR < 102.7. **CVE ID : CVE-2023-23603**	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://www.mozilla.org/security/advisories/mfsa2023-03/, https://www.mozilla.org/security/advisories/mfsa2023-02/, https://bugzilla.mozilla.org/show_bug.cgi?id=1800832	A-MOZ-FIRE-280623/350
N/A	02-Jun-2023	6.5	A duplicate <code>SystemPrincipal</code> object could be created when parsing a non-system html document via <code>DOMParser::ParseFromSafeString</code>. This could have lead to bypassing web	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://bugzilla.mozilla.org/show_bug.cgi?id=1802346	A-MOZ-FIRE-280623/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security checks. This vulnerability affects Firefox < 109. **CVE ID : CVE-2023-23604**		
Affected Version(s): * Up to (excluding) 110.0					
N/A	02-Jun-2023	8.8	An attacker could construct a PKCS 12 cert bundle in such a way that could allow for arbitrary memory writes via PKCS 12 Safe Bag attributes being mishandled. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-0767**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://bugzilla.mozilla.org/show_bug.cgi?id=1804640, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/352
N/A	02-Jun-2023	8.8	Permission prompts for opening external schemes were only shown for <code>ContentPrincipals</code> resulting in extensions being able to open them without user interaction via <code>ExpandedPrincipals</code>. This could lead to further malicious actions such as downloading files or interacting with software already installed on the	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25729**		
N/A	02-Jun-2023	8.8	Due to URL previews in the network panel of developer tools improperly storing URLs, query parameters could potentially be used to overwrite global objects in privileged code. This vulnerability affects Firefox < 110. **CVE ID : CVE-2023-25731**	https://www.mozilla.org/security/advisories/mfsa2023-05/	A-MOZ-FIRE-280623/354
Out-of-bounds Write	02-Jun-2023	8.8	When encoding data from an <code>inputStream</code> in <code>xpcom</code> the size of the input being encoded was not correctly calculated potentially leading to an out of bounds memory write. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25732**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/355
Use After Free	02-Jun-2023	8.8	Cross-compartment wrappers wrapping a	https://www.mozilla.org/se	A-MOZ-FIRE-280623/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripted proxy could have caused objects from other compartments to be stored in the main compartment resulting in a use-after-free after unwrapping the proxy. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25735**	curity/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	
N/A	02-Jun-2023	8.8	An invalid downcast from <code>nsTextNode</code> to <code>SVGElement</code> could have lead to undefined behavior. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25737**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/357
Use After Free	02-Jun-2023	8.8	Module load requests that failed were not being checked as to whether or not they were cancelled causing a use-after-free in <code>ScriptLoadContext</code>. This vulnerability affects Firefox < 110,	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.	A-MOZ-FIRE-280623/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25739**	mozilla.org/security/advisories/mfsa2023-06/	
N/A	02-Jun-2023	8.8	After downloading a Windows <code>.scf</code> script from the local filesystem, an attacker could supply a remote path that would lead to unexpected network requests from the operating system. This also had the potential to leak NTLM credentials to the resource. *This bug only affects Firefox for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 110. **CVE ID : CVE-2023-25740**	https://www.mozilla.org/security/advisories/mfsa2023-05/	A-MOZ-FIRE-280623/359
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers Kershaw Chang and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 109 and Firefox ESR 102.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			run arbitrary code. This vulnerability affects Firefox < 110 and Firefox ESR < 102.8. **CVE ID : CVE-2023-25744**		
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers Timothy Nikkel, Gabriele Svelto, Jeff Muizelaar and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 109. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 110. **CVE ID : CVE-2023-25745**	https://bugzilla.mozilla.org/buglist.cgi?bug_id=1688592%2C1797186%2C1804998%2C1806521%2C1813284, https://www.mozilla.org/security/advisories/mfsa2023-05/	A-MOZ-FIRE-280623/361
N/A	02-Jun-2023	8.1	After downloading a Windows <code>.url</code> shortcut from the local filesystem, an attacker could supply a remote path that would lead to unexpected network requests from the operating system. This also had the potential to leak NTLM credentials to the resource. *This bug only affects	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/, https://bugzil	A-MOZ-FIRE-280623/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25734**	la.mozilla.org/show_bug.cgi?id=1784451	
N/A	02-Jun-2023	6.5	The <code>Content-Security-Policy-Report-Only</code> header could allow an attacker to leak a child iframe's unredacted URI when interaction with that iframe triggers a redirect. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25728**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/363
Out-of-bounds Read	02-Jun-2023	6.5	Members of the <code>DEVMODEW</code> struct set by the printer device driver weren't being validated and could have resulted in invalid values which in turn would cause the browser to attempt out of bounds access to related variables. *This bug only affects Firefox on Windows. Other operating	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			systems are unaffected.*. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25738**		
N/A	02-Jun-2023	6.5	When dragging and dropping an image cross-origin, the image's size could potentially be leaked. This behavior was shipped in 109 and caused web compatibility problems as well as this security concern, so the behavior was disabled until further review. This vulnerability affects Firefox < 110. **CVE ID : CVE-2023-25741**	https://bugzilla.mozilla.org/show_bug.cgi?id=1437126, https://www.mozilla.org/security/advisories/mfsa2023-05/, https://bugzilla.mozilla.org/show_bug.cgi?id=1812611	A-MOZ-FIRE-280623/365
N/A	02-Jun-2023	6.5	When importing a SPKI RSA public key as ECDSA P-256, the key would be handled incorrectly causing the tab to crash. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25742**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jun-2023	5.4	A background script invoking <code>requestFullscreen</code> and then blocking the main thread could force the browser into fullscreen mode indefinitely, resulting in potential user confusion or spoofing attacks. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25730**	https://bugzilla.mozilla.org/show_bug.cgi?id=1794622, https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/367
Affected Version(s): * Up to (excluding) 111.0					
Improper Preservation of Permissions	02-Jun-2023	8.8	If temporary "one-time" permissions, such as the ability to use the Camera, were granted to a document loaded using a file: URL, that permission persisted in that tab for all other documents loaded from a file: URL. This is potentially dangerous if the local files came from different sources, such as in a download directory. This vulnerability affects Firefox < 111. **CVE ID : CVE-2023-28161**	https://bugzilla.mozilla.org/show_bug.cgi?id=1811181, https://www.mozilla.org/security/advisories/mfsa2023-09/	A-MOZ-FIRE-280623/368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-Jun-2023	8.8	While implementing AudioWorklets, some code may have casted one type to another, invalid, dynamic type. This could have led to a potentially exploitable crash. This vulnerability affects Firefox < 111, Firefox ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-28162**	https://www.mozilla.org/security/advisories/mfsa2023-11/, https://www.mozilla.org/security/advisories/mfsa2023-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/, https://bugzilla.mozilla.org/show_bug.cgi?id=1811327	A-MOZ-FIRE-280623/369
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers Timothy Nikkel, Andrew McCreight, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 110 and Firefox ESR 102.8. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 111, Firefox ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-28176**	https://www.mozilla.org/security/advisories/mfsa2023-11/, https://www.mozilla.org/security/advisories/mfsa2023-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/	A-MOZ-FIRE-280623/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers and community members Calixte Denizet, Gabriele Svelto, Andrew McCreight, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 110. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 111. **CVE ID : CVE-2023-28177**	https://bugzilla.mozilla.org/buglist.cgi?bug_id=1803109%2C1808832%2C1809542%2C1817336, https://www.mozilla.org/security/advisories/mfsa2023-09/	A-MOZ-FIRE-280623/371
N/A	02-Jun-2023	6.5	Sometimes, when invalidating JIT code while following an iterator, the newly generated code could be overwritten incorrectly. This could lead to a potentially exploitable crash. This vulnerability affects Firefox < 111, Firefox ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-25751**	https://www.mozilla.org/security/advisories/mfsa2023-11/, https://www.mozilla.org/security/advisories/mfsa2023-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/, https://bugzilla.mozilla.org/show_bug.cgi?id=1814899	A-MOZ-FIRE-280623/372
N/A	02-Jun-2023	6.5	When accessing throttled streams, the	https://www.mozilla.org/se	A-MOZ-FIRE-280623/373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			count of available bytes needed to be checked in the calling function to be within bounds. This may have lead future code to be incorrect and vulnerable. This vulnerability affects Firefox < 111, Firefox ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-25752**	curity/advisories/mfsa2023-11/, https://bugzilla.mozilla.org/show_bug.cgi?id=1811627, https://www.mozilla.org/security/advisories/mfsa2023-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/	
N/A	02-Jun-2023	6.5	When following a redirect to a publicly accessible web extension file, the URL may have been translated to the actual local path, leaking potentially sensitive information. This vulnerability affects Firefox < 111. **CVE ID : CVE-2023-28160**	https://bugzilla.mozilla.org/show_bug.cgi?id=1802385, https://www.mozilla.org/security/advisories/mfsa2023-09/	A-MOZ-FIRE-280623/374
N/A	02-Jun-2023	6.5	When downloading files through the Save As dialog on Windows with suggested filenames containing environment variable names, Windows would have resolved those in the context of the current user. *This bug only affects Firefox on Windows. Other	https://www.mozilla.org/security/advisories/mfsa2023-11/, https://bugzilla.mozilla.org/show_bug.cgi?id=1817768, https://www.mozilla.org/security/advisories/mfsa202	A-MOZ-FIRE-280623/375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions of Firefox are unaffected.*. This vulnerability affects Firefox < 111, Firefox ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-28163**	3-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/	
N/A	02-Jun-2023	6.5	Dragging a URL from a cross-origin iframe that was removed during the drag could have led to user confusion and website spoofing attacks. This vulnerability affects Firefox < 111, Firefox ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-28164**	https://www.mozilla.org/security/advisories/mfsa2023-11/, https://bugzilla.mozilla.org/show_bug.cgi?id=1809122, https://www.mozilla.org/security/advisories/mfsa2023-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/	A-MOZ-FIRE-280623/376
N/A	02-Jun-2023	4.3	By displaying a prompt with a long description, the fullscreen notification could have been hidden, resulting in potential user confusion or spoofing attacks. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 111.	https://www.mozilla.org/security/advisories/mfsa2023-09/, https://bugzilla.mozilla.org/show_bug.cgi?id=1798798	A-MOZ-FIRE-280623/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25748		
N/A	02-Jun-2023	4.3	Android applications with unpatched vulnerabilities can be launched from a browser using Intents, exposing users to these vulnerabilities. Firefox will now confirm with users that they want to launch an external application before doing so. *This bug only affects Firefox for Android. Other versions of Firefox are unaffected.*. This vulnerability affects Firefox < 111. **CVE ID : CVE-2023-25749**	https://bugzilla.mozilla.org/show_bug.cgi?id=1810705, https://www.mozilla.org/security/advisories/mfsa2023-09/	A-MOZ-FIRE-280623/378
Exposure of Resource to Wrong Sphere	02-Jun-2023	4.3	Under certain circumstances, a ServiceWorker's offline cache may have leaked to the file system when using private browsing mode. This vulnerability affects Firefox < 111. **CVE ID : CVE-2023-25750**	https://www.mozilla.org/security/advisories/mfsa2023-09/, https://bugzilla.mozilla.org/show_bug.cgi?id=1814733	A-MOZ-FIRE-280623/379
N/A	02-Jun-2023	4.3	The fullscreen notification could have been hidden on Firefox for Android by using download popups, resulting in	https://www.mozilla.org/security/advisories/mfsa2023-09/, https://bugzil	A-MOZ-FIRE-280623/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential user confusion or spoofing attacks. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 111. **CVE ID : CVE-2023-28159**	la.mozilla.org/show_bug.cgi?id=1783561	
Affected Version(s): * Up to (excluding) 112.0					
Use After Free	02-Jun-2023	8.8	An attacker could cause the memory manager to incorrectly free a pointer that addresses attacker-controlled memory, resulting in an assertion, memory corruption, or a potentially exploitable crash. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29536**	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1821959, https://www.mozilla.org/security/advisories/mfsa2023-15/	A-MOZ-FIRE-280623/381
Improper Encoding or Escaping of Output	02-Jun-2023	8.8	Firefox did not properly handle downloads of files ending in <code>.desktop</code>, which can be interpreted to run attacker-controlled commands. *This bug only affects	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/,	A-MOZ-FIRE-280623/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox for Linux on certain Distributions. Other operating systems are unaffected, and Mozilla is unable to enumerate all affected Linux Distributions.*. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29541**	https://bugzilla.mozilla.org/show_bug.cgi?id=1810191, https://www.mozilla.org/security/advisories/mfsa2023-15/	
Use After Free	02-Jun-2023	8.8	An attacker could have caused memory corruption and a potentially exploitable use-after-free of a pointer in a global object's debugger vector. This vulnerability affects Firefox for Android < 112, Firefox < 112, and Focus for Android < 112. **CVE ID : CVE-2023-29543**	https://www.mozilla.org/security/advisories/mfsa2023-13/	A-MOZ-FIRE-280623/383
N/A	02-Jun-2023	8.8	Mozilla developers Randell Jesup, Andrew Osmond, Sebastian Hengst, Andrew McCreight, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 111 and Firefox ESR 102.9. Some of these bugs	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://www.	A-MOZ-FIRE-280623/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29550**	mozilla.org/security/advisories/mfsa2023-15/	
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers Randell Jesup, Andrew McCreight, Gabriele Svelto, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 111. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox for Android < 112, Firefox < 112, and Focus for Android < 112. **CVE ID : CVE-2023-29551**	https://www.mozilla.org/security/advisories/mfsa2023-13/	A-MOZ-FIRE-280623/385
Concurrent Execution using Shared	02-Jun-2023	7.5	Multiple race conditions in the font initialization could have led to memory	https://www.mozilla.org/security/adviso	A-MOZ-FIRE-280623/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			corruption and execution of attacker-controlled code. This vulnerability affects Firefox for Android < 112, Firefox < 112, and Focus for Android < 112. **CVE ID : CVE-2023-29537**	ries/mfsa2023-13/	
N/A	02-Jun-2023	6.5	A website could have obscured the fullscreen notification by using a combination of <code>window.open</code>, fullscreen requests, <code>window.name</code> assignments, and <code>setInterval</code> calls. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29533**	https://bugzilla.mozilla.org/show_bug.cgi?id=1814597, https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1798219	A-MOZ-FIRE-280623/387
N/A	02-Jun-2023	6.5	Following a Garbage Collector compaction, weak maps may have been accessed before they were correctly traced. This resulted in memory corruption	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/se	A-MOZ-FIRE-280623/388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and a potentially exploitable crash. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29535**	curity/advisories/mfsa2023-13/, https://www.mozilla.org/security/advisories/mfsa2023-15/	
NULL Pointer Dereference	02-Jun-2023	6.5	When handling the filename directive in the Content-Disposition header, the filename would be truncated if the filename contained a NULL character. This could have led to reflected file download attacks potentially tricking users to install malware. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29539**	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://www.mozilla.org/security/advisories/mfsa2023-15/	A-MOZ-FIRE-280623/389
Uncontrolled Resource Consumption	02-Jun-2023	6.5	If multiple instances of resource exhaustion occurred at the incorrect time, the garbage collector could have caused memory corruption and a potentially exploitable crash. This	https://www.mozilla.org/security/advisories/mfsa2023-13/	A-MOZ-FIRE-280623/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects Firefox for Android < 112, Firefox < 112, and Focus for Android < 112. **CVE ID : CVE-2023-29544**		
N/A	02-Jun-2023	6.5	When a secure cookie existed in the Firefox cookie jar an insecure cookie for the same domain could have been created, when it should have silently failed. This could have led to a desynchronization in expected results when reading from the secure cookie. This vulnerability affects Firefox for Android < 112, Firefox < 112, and Focus for Android < 112. **CVE ID : CVE-2023-29547**	https://www.mozilla.org/security/advisories/mfsa2023-13/	A-MOZ-FIRE-280623/391
N/A	02-Jun-2023	6.5	A wrong lowering instruction in the ARM64 Ion compiler resulted in a wrong optimization result. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29548**	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://www.mozilla.org/security/advisories/mfsa2023-15/, https://bugzil	A-MOZ-FIRE-280623/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				la.mozilla.org/show_bug.cgi?id=1822754	
Inadequate Encryption Strength	02-Jun-2023	6.5	Under certain circumstances, a call to the <code>bind</code> function may have resulted in the incorrect realm. This may have created a vulnerability relating to JavaScript-implemented sandboxes such as SES. This vulnerability affects Firefox for Android < 112, Firefox < 112, and Focus for Android < 112. **CVE ID : CVE-2023-29549**	https://www.mozilla.org/security/advisories/mfsa2023-13/	A-MOZ-FIRE-280623/393
URL Redirection to Untrusted Site ('Open Redirect')	02-Jun-2023	6.1	Using a redirect embedded into <code>sourceMappingUrls</code> could allow for navigation to external protocol links in sandboxed iframes without <code>allow-top-navigation-to-custom-protocols</code>. This vulnerability affects Firefox for Android < 112, Firefox < 112, and Focus for Android < 112. **CVE ID : CVE-2023-29540**	https://www.mozilla.org/security/advisories/mfsa2023-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1790542	A-MOZ-FIRE-280623/394
Exposure of	02-Jun-2023	5.3	Under specific circumstances a	https://www.mozilla.org/se	A-MOZ-FIRE-280623/395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			WebExtension may have received a <code>jar:file:///</code> URI instead of a <code>moz-extension:///</code> URI during a load request. This leaked directory paths on the user's machine. This vulnerability affects Firefox for Android < 112, Firefox < 112, and Focus for Android < 112. **CVE ID : CVE-2023-29538**	curity/advisories/mfsa2023-13/	
Affected Version(s): * Up to (excluding) 113.0					
Use of Uninitialized Resource	02-Jun-2023	8.8	When reading a file, an uninitialized value could have been used as read limit. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32213**	https://www.mozilla.org/security/advisories/mfsa2023-16/, https://bugzilla.mozilla.org/show_bug.cgi?id=1826666, https://www.mozilla.org/security/advisories/mfsa2023-18/, https://www.mozilla.org/security/advisories/mfsa2023-17/	A-MOZ-FIRE-280623/396
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers and community members Gabriele Svelto, Andrew Osmond, Emily McDonough, Sebastian	https://www.mozilla.org/security/advisories/mfsa2023-16/, https://www.	A-MOZ-FIRE-280623/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hengst, Andrew McCreight and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 112 and Firefox ESR 102.10. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32215**	mozilla.org/security/advisories/mfsa2023-18/, https://www.mozilla.org/security/advisories/mfsa2023-17/	
N/A	02-Jun-2023	6.5	In multiple cases browser prompts could have been obscured by popups controlled by content. These could have led to potential user confusion and spoofing attacks. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32205**	https://bugzilla.mozilla.org/show_bug.cgi?id=1753341, https://bugzilla.mozilla.org/show_bug.cgi?id=1753339, https://www.mozilla.org/security/advisories/mfsa2023-16/, https://www.mozilla.org/security/advisories/mfsa2023-18/	A-MOZ-FIRE-280623/398
Out-of-bounds Read	02-Jun-2023	6.5	An out-of-bound read could have led to a crash in the RLBox	https://bugzilla.mozilla.org/show_bug.cgi	A-MOZ-FIRE-280623/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Expat driver. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32206**	?id=1824892, https://www.mozilla.org/security/advisories/mfsa2023-16/, https://www.mozilla.org/security/advisories/mfsa2023-18/, https://www.mozilla.org/security/advisories/mfsa2023-17/	
Authentication Bypass by Spoofing	02-Jun-2023	6.5	A missing delay in popup notifications could have made it possible for an attacker to trick a user into granting permissions. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32207**	https://www.mozilla.org/security/advisories/mfsa2023-16/, https://bugzilla.mozilla.org/show_bug.cgi?id=1826116, https://www.mozilla.org/security/advisories/mfsa2023-18/, https://www.mozilla.org/security/advisories/mfsa2023-17/	A-MOZ-FIRE-280623/400
N/A	02-Jun-2023	6.5	A type checking bug would have led to invalid code being compiled. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11.	https://www.mozilla.org/security/advisories/mfsa2023-16/, https://www.mozilla.org/security/adviso	A-MOZ-FIRE-280623/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32211	ries/mfsa2023-18/, https://bugzilla.mozilla.org/show_bug.cgi?id=1823379, https://www.mozilla.org/security/advisories/mfsa2023-17/	
N/A	02-Jun-2023	4.3	An attacker could have positioned a <code>datalist</code> element to obscure the address bar. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32212**	https://www.mozilla.org/security/advisories/mfsa2023-16/, https://bugzilla.mozilla.org/show_bug.cgi?id=1826622, https://www.mozilla.org/security/advisories/mfsa2023-18/, https://www.mozilla.org/security/advisories/mfsa2023-17/	A-MOZ-FIRE-280623/402
Product: firefox_esr					
Affected Version(s): * Up to (excluding) 102.10					
Use After Free	02-Jun-2023	8.8	An attacker could cause the memory manager to incorrectly free a pointer that addresses attacker-controlled memory, resulting in an assertion, memory corruption, or a potentially exploitable crash. This	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://bugzil	A-MOZ-FIRE-280623/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29536**	la.mozilla.org/show_bug.cgi?id=1821959, https://www.mozilla.org/security/advisories/mfsa2023-15/	
Improper Encoding or Escaping of Output	02-Jun-2023	8.8	Firefox did not properly handle downloads of files ending in <code>.desktop</code>, which can be interpreted to run attacker-controlled commands. *This bug only affects Firefox for Linux on certain Distributions. Other operating systems are unaffected, and Mozilla is unable to enumerate all affected Linux Distributions.*. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29541**	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1810191, https://www.mozilla.org/security/advisories/mfsa2023-15/	A-MOZ-FIRE-280623/404
N/A	02-Jun-2023	8.8	Mozilla developers Randell Jesup, Andrew Osmond, Sebastian Hengst, Andrew McCreight, and the Mozilla Fuzzing Team reported memory	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/se	A-MOZ-FIRE-280623/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			safety bugs present in Firefox 111 and Firefox ESR 102.9. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29550**	curity/advisories/mfsa2023-13/, https://www.mozilla.org/security/advisories/mfsa2023-15/	
Out-of-bounds Write	02-Jun-2023	6.5	Unexpected data returned from the Safe Browsing API could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 102.10 and Firefox ESR < 102.10. **CVE ID : CVE-2023-1945**	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://bugzilla.mozilla.org/show_bug.cgi?id=1777588, https://www.mozilla.org/security/advisories/mfsa2023-15/	A-MOZ-FIRE-280623/406
N/A	02-Jun-2023	6.5	A website could have obscured the fullscreen notification by using a combination of <code>window.open</code>, fullscreen requests, <code>window.name<	https://bugzilla.mozilla.org/show_bug.cgi?id=1814597, https://www.mozilla.org/security/advisories/mfsa2023-14/,	A-MOZ-FIRE-280623/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/code> assignments, and <code>setInterval</code> calls. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29533**	https://www.mozilla.org/security/advisories/mfsa2023-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1798219	
N/A	02-Jun-2023	6.5	Following a Garbage Collector compaction, weak maps may have been accessed before they were correctly traced. This resulted in memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29535**	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://www.mozilla.org/security/advisories/mfsa2023-15/	A-MOZ-FIRE-280623/408
NULL Pointer Dereference	02-Jun-2023	6.5	When handling the filename directive in the Content-Disposition header, the filename would be truncated if the filename contained a NULL character. This	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/adviso	A-MOZ-FIRE-280623/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could have led to reflected file download attacks potentially tricking users to install malware. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29539**	ries/mfsa2023-13/, https://www.mozilla.org/security/advisories/mfsa2023-15/	
N/A	02-Jun-2023	6.5	When a secure cookie existed in the Firefox cookie jar an insecure cookie for the same domain could have been created, when it should have silently failed. This could have led to a desynchronization in expected results when reading from the secure cookie. This vulnerability affects Firefox for Android < 112, Firefox < 112, and Focus for Android < 112. **CVE ID : CVE-2023-29547**	https://www.mozilla.org/security/advisories/mfsa2023-13/	A-MOZ-FIRE-280623/410
N/A	02-Jun-2023	6.5	A wrong lowering instruction in the ARM64 Ion compiler resulted in a wrong optimization result. This vulnerability affects Firefox < 112, Focus for Android <	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/adviso	A-MOZ-FIRE-280623/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29548**	ries/mfsa2023-13/, https://www.mozilla.org/security/advisories/mfsa2023-15/, https://bugzilla.mozilla.org/show_bug.cgi?id=1822754	
Affected Version(s): * Up to (excluding) 102.11					
Use of Uninitialized Resource	02-Jun-2023	8.8	When reading a file, an uninitialized value could have been used as read limit. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32213**	https://www.mozilla.org/security/advisories/mfsa2023-16/, https://bugzilla.mozilla.org/show_bug.cgi?id=1826666, https://www.mozilla.org/security/advisories/mfsa2023-18/, https://www.mozilla.org/security/advisories/mfsa2023-17/	A-MOZ-FIRE-280623/412
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers and community members Gabriele Svelto, Andrew Osmond, Emily McDonough, Sebastian Hengst, Andrew McCreight and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 112 and	https://www.mozilla.org/security/advisories/mfsa2023-16/, https://www.mozilla.org/security/advisories/mfsa2023-18/, https://www.mozilla.org/se	A-MOZ-FIRE-280623/413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox ESR 102.10. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32215**	curity/advisories/mfsa2023-17/	
N/A	02-Jun-2023	6.5	In multiple cases browser prompts could have been obscured by popups controlled by content. These could have led to potential user confusion and spoofing attacks. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32205**	https://bugzilla.mozilla.org/show_bug.cgi?id=1753341, https://bugzilla.mozilla.org/show_bug.cgi?id=1753339, https://www.mozilla.org/security/advisories/mfsa2023-16/, https://www.mozilla.org/security/advisories/mfsa2023-18/	A-MOZ-FIRE-280623/414
Out-of-bounds Read	02-Jun-2023	6.5	An out-of-bound read could have led to a crash in the RLBox Expat driver. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11.	https://bugzilla.mozilla.org/show_bug.cgi?id=1824892, https://www.mozilla.org/security/advisories/mfsa2023-16/,	A-MOZ-FIRE-280623/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32206	https://www.mozilla.org/security/advisories/mfsa2023-18/, https://www.mozilla.org/security/advisories/mfsa2023-17/	
Authentication Bypass by Spoofing	02-Jun-2023	6.5	A missing delay in popup notifications could have made it possible for an attacker to trick a user into granting permissions. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32207**	https://www.mozilla.org/security/advisories/mfsa2023-16/, https://bugzilla.mozilla.org/show_bug.cgi?id=1826116, https://www.mozilla.org/security/advisories/mfsa2023-18/, https://www.mozilla.org/security/advisories/mfsa2023-17/	A-MOZ-FIRE-280623/416
N/A	02-Jun-2023	6.5	A type checking bug would have led to invalid code being compiled. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32211**	https://www.mozilla.org/security/advisories/mfsa2023-16/, https://www.mozilla.org/security/advisories/mfsa2023-18/, https://bugzilla.mozilla.org/show_bug.cgi?id=1823379,	A-MOZ-FIRE-280623/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://www.mozilla.org/security/advisories/mfsa2023-17/	
N/A	02-Jun-2023	4.3	An attacker could have positioned a <code>datalist</code> element to obscure the address bar. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32212**	https://www.mozilla.org/security/advisories/mfsa2023-16/, https://bugzilla.mozilla.org/show_bug.cgi?id=1826622, https://www.mozilla.org/security/advisories/mfsa2023-18/, https://www.mozilla.org/security/advisories/mfsa2023-17/	A-MOZ-FIRE-280623/418
Affected Version(s): * Up to (excluding) 102.7					
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 108 and Firefox ESR 102.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 109, Thunderbird < 102.7,	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://www.mozilla.org/security/advisories/mfsa2023-03/, https://www.mozilla.org/security/advisories/mfsa2023-02/	A-MOZ-FIRE-280623/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Firefox ESR < 102.7. **CVE ID : CVE-2023-23605**		
N/A	02-Jun-2023	6.5	Due to the Firefox GTK wrapper code's use of text/plain for drag data and GTK treating all text/plain MIMEs containing file URLs as being dragged a website could arbitrarily read a file via a call to <code>DataTransfer.setData</code>. This vulnerability affects Firefox < 109, Thunderbird < 102.7, and Firefox ESR < 102.7. **CVE ID : CVE-2023-23598**	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://www.mozilla.org/security/advisories/mfsa2023-03/, https://www.mozilla.org/security/advisories/mfsa2023-02/, https://bugzilla.mozilla.org/show_bug.cgi?id=1800425	A-MOZ-FIRE-280623/420
Improper Encoding or Escaping of Output	02-Jun-2023	6.5	When copying a network request from the developer tools panel as a curl command the output was not being properly sanitized and could allow arbitrary commands to be hidden within. This vulnerability affects Firefox < 109, Thunderbird < 102.7, and Firefox ESR < 102.7. **CVE ID : CVE-2023-23599**	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://www.mozilla.org/security/advisories/mfsa2023-03/, https://www.mozilla.org/security/advisories/mfsa2023-02/, https://bugzilla.mozilla.org/show_bug.cgi?id=1777800	A-MOZ-FIRE-280623/421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Origin Validation Error	02-Jun-2023	6.5	Navigations were being allowed when dragging a URL from a cross-origin iframe into the same tab which could lead to website spoofing attacks. This vulnerability affects Firefox < 109, Thunderbird < 102.7, and Firefox ESR < 102.7. **CVE ID : CVE-2023-23601**	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://www.mozilla.org/security/advisories/mfsa2023-03/, https://bugzilla.mozilla.org/show_bug.cgi?id=1794268, https://www.mozilla.org/security/advisories/mfsa2023-02/	A-MOZ-FIRE-280623/422
Improper Check for Unusual or Exceptional Conditions	02-Jun-2023	6.5	A mishandled security check when creating a WebSocket in a WebWorker caused the Content Security Policy connect-src header to be ignored. This could lead to connections to restricted origins from inside WebWorkers. This vulnerability affects Firefox < 109, Thunderbird < 102.7, and Firefox ESR < 102.7. **CVE ID : CVE-2023-23602**	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://www.mozilla.org/security/advisories/mfsa2023-03/, https://www.mozilla.org/security/advisories/mfsa2023-02/, https://bugzilla.mozilla.org/show_bug.cgi?id=1800890	A-MOZ-FIRE-280623/423
N/A	02-Jun-2023	6.5	Regular expressions used to filter out forbidden properties and values from style directives in calls to	https://www.mozilla.org/security/advisories/mfsa2023-01/,	A-MOZ-FIRE-280623/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<code>console.log</code> weren't accounting for external URLs. Data could then be potentially exfiltrated from the browser. This vulnerability affects Firefox < 109, Thunderbird < 102.7, and Firefox ESR < 102.7. **CVE ID : CVE-2023-23603**	https://www.mozilla.org/security/advisories/mfsa2023-03/, https://www.mozilla.org/security/advisories/mfsa2023-02/, https://bugzilla.mozilla.org/show_bug.cgi?id=1800832	
Affected Version(s): * Up to (excluding) 102.8					
N/A	02-Jun-2023	8.8	An attacker could construct a PKCS 12 cert bundle in such a way that could allow for arbitrary memory writes via PKCS 12 Safe Bag attributes being mishandled. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-0767**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://bugzilla.mozilla.org/show_bug.cgi?id=1804640, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/425
N/A	02-Jun-2023	8.8	Permission prompts for opening external schemes were only shown for <code>ContentPrincipals</code> resulting in extensions being able to open them without user	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa202	A-MOZ-FIRE-280623/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction via <code>ExpandedPrincipals</code>. This could lead to further malicious actions such as downloading files or interacting with software already installed on the system. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25729**	3-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	
Out-of-bounds Write	02-Jun-2023	8.8	When encoding data from an <code>inputStream</code> in <code>xpcom</code> the size of the input being encoded was not correctly calculated potentially leading to an out of bounds memory write. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25732**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/427
Use After Free	02-Jun-2023	8.8	Cross-compartment wrappers wrapping a scripted proxy could have caused objects from other compartments to be stored in the main compartment	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/adviso	A-MOZ-FIRE-280623/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a use-after-free after unwrapping the proxy. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25735**	ries/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	
N/A	02-Jun-2023	8.8	An invalid downcast from <code>nsTextNode</code> to <code>SVGElement</code> could have lead to undefined behavior. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25737**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/429
Use After Free	02-Jun-2023	8.8	Module load requests that failed were not being checked as to whether or not they were cancelled causing a use-after-free in <code>ScriptLoadContext</code>. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25739**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers Kershaw Chang and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 109 and Firefox ESR 102.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 110 and Firefox ESR < 102.8. **CVE ID : CVE-2023-25744**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/431
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers Philipp and Gabriele Svelto reported memory safety bugs present in Firefox ESR 102.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 102.8 and Firefox ESR < 102.8. **CVE ID : CVE-2023-25746**	https://bugzilla.mozilla.org/buglist.cgi?bug_id=1544127%2C1762368, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/432
N/A	02-Jun-2023	8.1	After downloading a Windows <code>.url</code>	https://www.mozilla.org/security/adviso	A-MOZ-FIRE-280623/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			shortcut from the local filesystem, an attacker could supply a remote path that would lead to unexpected network requests from the operating system. This also had the potential to leak NTLM credentials to the resource. *This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25734**	ries/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/, https://bugzilla.mozilla.org/show_bug.cgi?id=1784451	
N/A	02-Jun-2023	6.5	The <code>Content-Security-Policy-Report-Only</code> header could allow an attacker to leak a child iframe's unredacted URI when interaction with that iframe triggers a redirect. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25728**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jun-2023	6.5	Members of the <code>DEVMODEW</code> struct set by the printer device driver weren't being validated and could have resulted in invalid values which in turn would cause the browser to attempt out of bounds access to related variables. *This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25738**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/435
N/A	02-Jun-2023	6.5	When importing a SPKI RSA public key as ECDSA P-256, the key would be handled incorrectly causing the tab to crash. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25742**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/436
N/A	02-Jun-2023	5.4	A background script invoking <code>requestFullscr	https://bugzilla.mozilla.org/show_bug.cgi	A-MOZ-FIRE-280623/437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			een</code> and then blocking the main thread could force the browser into fullscreen mode indefinitely, resulting in potential user confusion or spoofing attacks. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25730**	?id=1794622, https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	
Affected Version(s): * Up to (excluding) 102.9					
Incorrect Type Conversion or Cast	02-Jun-2023	8.8	While implementing AudioWorklets, some code may have casted one type to another, invalid, dynamic type. This could have led to a potentially exploitable crash. This vulnerability affects Firefox < 111, Firefox ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-28162**	https://www.mozilla.org/security/advisories/mfsa2023-11/, https://www.mozilla.org/security/advisories/mfsa2023-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/, https://bugzilla.mozilla.org/show_bug.cgi?id=1811327	A-MOZ-FIRE-280623/438
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers Timothy Nikkel, Andrew McCreight, and the Mozilla Fuzzing Team reported memory safety bugs present in	https://www.mozilla.org/security/advisories/mfsa2023-11/, https://www.mozilla.org/se	A-MOZ-FIRE-280623/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox 110 and Firefox ESR 102.8. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 111, Firefox ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-28176**	curity/advisories/mfsa2023-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/	
N/A	02-Jun-2023	6.5	Sometimes, when invalidating JIT code while following an iterator, the newly generated code could be overwritten incorrectly. This could lead to a potentially exploitable crash. This vulnerability affects Firefox < 111, Firefox ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-25751**	https://www.mozilla.org/security/advisories/mfsa2023-11/, https://www.mozilla.org/security/advisories/mfsa2023-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/, https://bugzilla.mozilla.org/show_bug.cgi?id=1814899	A-MOZ-FIRE-280623/440
N/A	02-Jun-2023	6.5	When accessing throttled streams, the count of available bytes needed to be checked in the calling function to be within bounds. This may	https://www.mozilla.org/security/advisories/mfsa2023-11/, https://bugzilla.mozilla.org	A-MOZ-FIRE-280623/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have lead future code to be incorrect and vulnerable. This vulnerability affects Firefox < 111, Firefox ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-25752**	/show_bug.cgi?id=1811627, https://www.mozilla.org/security/advisories/mfsa2023-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/	
N/A	02-Jun-2023	6.5	When downloading files through the Save As dialog on Windows with suggested filenames containing environment variable names, Windows would have resolved those in the context of the current user. *This bug only affects Firefox on Windows. Other versions of Firefox are unaffected.*. This vulnerability affects Firefox < 111, Firefox ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-28163**	https://www.mozilla.org/security/advisories/mfsa2023-11/, https://bugzilla.mozilla.org/show_bug.cgi?id=1817768, https://www.mozilla.org/security/advisories/mfsa2023-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/	A-MOZ-FIRE-280623/442
N/A	02-Jun-2023	6.5	Dragging a URL from a cross-origin iframe that was removed during the drag could have led to user confusion and website spoofing attacks. This vulnerability affects Firefox < 111, Firefox	https://www.mozilla.org/security/advisories/mfsa2023-11/, https://bugzilla.mozilla.org/show_bug.cgi?id=1809122, https://www.	A-MOZ-FIRE-280623/443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-28164**	mozilla.org/security/advisories/mfsa2023-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/	
Product: firefox_focus					
Affected Version(s): -					
Authentication Bypass by Spoofing	02-Jun-2023	7.5	A lack of in app notification for entering fullscreen mode could have lead to a malicious website spoofing browser chrome. *This bug only affects Firefox Focus. Other versions of Firefox are unaffected.*. This vulnerability affects Firefox < 110 and Firefox ESR < 102.8. **CVE ID : CVE-2023-25743**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-FIRE-280623/444
Product: focus					
Affected Version(s): * Up to (excluding) 112.0					
Use After Free	02-Jun-2023	8.8	An attacker could cause the memory manager to incorrectly free a pointer that addresses attacker-controlled memory, resulting in an assertion, memory corruption, or a potentially exploitable crash. This vulnerability affects Firefox < 112, Focus	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://bugzilla.mozilla.org/show_bug.cgi	A-MOZ-FOCU-280623/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29536**	?id=1821959, https://www.mozilla.org/security/advisories/mfsa2023-15/	
Improper Encoding or Escaping of Output	02-Jun-2023	8.8	Firefox did not properly handle downloads of files ending in <code>.desktop</code>, which can be interpreted to run attacker-controlled commands. *This bug only affects Firefox for Linux on certain Distributions. Other operating systems are unaffected, and Mozilla is unable to enumerate all affected Linux Distributions.*. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29541**	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1810191, https://www.mozilla.org/security/advisories/mfsa2023-15/	A-MOZ-FOCU-280623/446
Use After Free	02-Jun-2023	8.8	An attacker could have caused memory corruption and a potentially exploitable use-after-free of a pointer in a global object's debugger vector. This vulnerability affects	https://www.mozilla.org/security/advisories/mfsa2023-13/	A-MOZ-FOCU-280623/447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox for Android < 112, Firefox < 112, and Focus for Android < 112. **CVE ID : CVE-2023-29543**		
N/A	02-Jun-2023	8.8	Mozilla developers Randell Jesup, Andrew Osmond, Sebastian Hengst, Andrew McCreight, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 111 and Firefox ESR 102.9. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29550**	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://www.mozilla.org/security/advisories/mfsa2023-15/	A-MOZ-FOCU-280623/448
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers Randell Jesup, Andrew McCreight, Gabriele Svelto, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 111. Some of these bugs showed evidence of memory	https://www.mozilla.org/security/advisories/mfsa2023-13/	A-MOZ-FOCU-280623/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox for Android < 112, Firefox < 112, and Focus for Android < 112. **CVE ID : CVE-2023-29551**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jun-2023	7.5	Multiple race conditions in the font initialization could have led to memory corruption and execution of attacker-controlled code. This vulnerability affects Firefox for Android < 112, Firefox < 112, and Focus for Android < 112. **CVE ID : CVE-2023-29537**	https://www.mozilla.org/security/advisories/mfsa2023-13/	A-MOZ-FOCU-280623/450
N/A	02-Jun-2023	6.5	A website could have obscured the fullscreen notification by using a combination of <code>window.open</code>, fullscreen requests, <code>window.name</code> assignments, and <code>setInterval</code> calls. This could have led to user confusion and possible spoofing	https://bugzilla.mozilla.org/show_bug.cgi?id=1814597, https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://bugzilla.mozilla.org	A-MOZ-FOCU-280623/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29533**	/show_bug.cgi?id=1798219	
N/A	02-Jun-2023	6.5	Following a Garbage Collector compaction, weak maps may have been accessed before they were correctly traced. This resulted in memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29535**	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://www.mozilla.org/security/advisories/mfsa2023-15/	A-MOZ-FOCU-280623/452
NULL Pointer Dereference	02-Jun-2023	6.5	When handling the filename directive in the Content-Disposition header, the filename would be truncated if the filename contained a NULL character. This could have led to reflected file download attacks potentially tricking users to install malware. This vulnerability affects	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://www.mozilla.org/security/adviso	A-MOZ-FOCU-280623/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29539**	ries/mfsa2023-15/	
Uncontrolled Resource Consumption	02-Jun-2023	6.5	If multiple instances of resource exhaustion occurred at the incorrect time, the garbage collector could have caused memory corruption and a potentially exploitable crash. This vulnerability affects Firefox for Android < 112, Firefox < 112, and Focus for Android < 112. **CVE ID : CVE-2023-29544**	https://www.mozilla.org/security/advisories/mfsa2023-13/	A-MOZ-FOCU-280623/454
N/A	02-Jun-2023	6.5	When a secure cookie existed in the Firefox cookie jar an insecure cookie for the same domain could have been created, when it should have silently failed. This could have led to a desynchronization in expected results when reading from the secure cookie. This vulnerability affects Firefox for Android < 112, Firefox < 112, and Focus for Android < 112.	https://www.mozilla.org/security/advisories/mfsa2023-13/	A-MOZ-FOCU-280623/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29547		
N/A	02-Jun-2023	6.5	A wrong lowering instruction in the ARM64 Ion compiler resulted in a wrong optimization result. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29548**	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://www.mozilla.org/security/advisories/mfsa2023-15/, https://bugzilla.mozilla.org/show_bug.cgi?id=1822754	A-MOZ-FOCU-280623/456
Inadequate Encryption Strength	02-Jun-2023	6.5	Under certain circumstances, a call to the <code>bind</code> function may have resulted in the incorrect realm. This may have created a vulnerability relating to JavaScript-implemented sandboxes such as SES. This vulnerability affects Firefox for Android < 112, Firefox < 112, and Focus for Android < 112. **CVE ID : CVE-2023-29549**	https://www.mozilla.org/security/advisories/mfsa2023-13/	A-MOZ-FOCU-280623/457
URL Redirection to	02-Jun-2023	6.1	Using a redirect embedded into <code>sourceMapping	https://www.mozilla.org/security/adviso	A-MOZ-FOCU-280623/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Site ('Open Redirect')			Urls</code> could allow for navigation to external protocol links in sandboxed iframes without <code>allow-top-navigation-to-custom-protocols</code>. This vulnerability affects Firefox for Android < 112, Firefox < 112, and Focus for Android < 112. **CVE ID : CVE-2023-29540**	ries/mfsa2023-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1790542	
Exposure of Resource to Wrong Sphere	02-Jun-2023	5.3	Under specific circumstances a WebExtension may have received a <code>jar:file:///</code> URI instead of a <code>moz-extension:///</code> URI during a load request. This leaked directory paths on the user's machine. This vulnerability affects Firefox for Android < 112, Firefox < 112, and Focus for Android < 112. **CVE ID : CVE-2023-29538**	https://www.mozilla.org/security/advisories/mfsa2023-13/	A-MOZ-FOCU-280623/459
Product: thunderbird					
Affected Version(s): * Up to (excluding) 102.10					
Use After Free	02-Jun-2023	8.8	An attacker could cause the memory manager to incorrectly free a pointer that addresses attacker-controlled	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.	A-MOZ-THUN-280623/460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory, resulting in an assertion, memory corruption, or a potentially exploitable crash. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29536**	mozilla.org/security/advisories/mfsa2023-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1821959, https://www.mozilla.org/security/advisories/mfsa2023-15/	
Improper Encoding or Escaping of Output	02-Jun-2023	8.8	Firefox did not properly handle downloads of files ending in <code>.desktop</code>, which can be interpreted to run attacker-controlled commands. *This bug only affects Firefox for Linux on certain Distributions. Other operating systems are unaffected, and Mozilla is unable to enumerate all affected Linux Distributions.*. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29541**	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1810191, https://www.mozilla.org/security/advisories/mfsa2023-15/	A-MOZ-THUN-280623/461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jun-2023	8.8	Mozilla developers Randell Jesup, Andrew Osmond, Sebastian Hengst, Andrew McCreight, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 111 and Firefox ESR 102.9. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29550**	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://www.mozilla.org/security/advisories/mfsa2023-15/	A-MOZ-THUN-280623/462
Out-of-bounds Write	02-Jun-2023	6.5	Unexpected data returned from the Safe Browsing API could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 102.10 and Firefox ESR < 102.10. **CVE ID : CVE-2023-1945**	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://bugzilla.mozilla.org/show_bug.cgi?id=1777588, https://www.mozilla.org/security/advisories/mfsa2023-15/	A-MOZ-THUN-280623/463
N/A	02-Jun-2023	6.5	A website could have obscured the	https://bugzilla.mozilla.org	A-MOZ-THUN-280623/464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fullscreen notification by using a combination of <code>window.open</code>, fullscreen requests, <code>window.name</code> assignments, and <code>setInterval</code> calls. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29533**	/show_bug.cgi?id=1814597, https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1798219	
N/A	02-Jun-2023	6.5	Following a Garbage Collector compaction, weak maps may have been accessed before they were correctly traced. This resulted in memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29535**	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://www.mozilla.org/security/advisories/mfsa2023-15/	A-MOZ-THUN-280623/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jun-2023	6.5	When handling the filename directive in the Content-Disposition header, the filename would be truncated if the filename contained a NULL character. This could have led to reflected file download attacks potentially tricking users to install malware. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29539**	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://www.mozilla.org/security/advisories/mfsa2023-15/	A-MOZ-THUN-280623/466
N/A	02-Jun-2023	6.5	A wrong lowering instruction in the ARM64 Ion compiler resulted in a wrong optimization result. This vulnerability affects Firefox < 112, Focus for Android < 112, Firefox ESR < 102.10, Firefox for Android < 112, and Thunderbird < 102.10. **CVE ID : CVE-2023-29548**	https://www.mozilla.org/security/advisories/mfsa2023-14/, https://www.mozilla.org/security/advisories/mfsa2023-13/, https://www.mozilla.org/security/advisories/mfsa2023-15/, https://bugzilla.mozilla.org/show_bug.cgi?id=1822754	A-MOZ-THUN-280623/467
Affected Version(s): * Up to (excluding) 102.11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Uninitialized Resource	02-Jun-2023	8.8	When reading a file, an uninitialized value could have been used as read limit. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32213**	https://www.mozilla.org/security/advisories/mfsa2023-16/, https://bugzilla.mozilla.org/show_bug.cgi?id=1826666, https://www.mozilla.org/security/advisories/mfsa2023-18/, https://www.mozilla.org/security/advisories/mfsa2023-17/	A-MOZ-THUN-280623/468
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers and community members Gabriele Svelto, Andrew Osmond, Emily McDonough, Sebastian Hengst, Andrew McCreight and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 112 and Firefox ESR 102.10. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 113, Firefox ESR < 102.11,	https://www.mozilla.org/security/advisories/mfsa2023-16/, https://www.mozilla.org/security/advisories/mfsa2023-18/, https://www.mozilla.org/security/advisories/mfsa2023-17/	A-MOZ-THUN-280623/469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Thunderbird < 102.11. **CVE ID : CVE-2023-32215**		
N/A	02-Jun-2023	6.5	In multiple cases browser prompts could have been obscured by popups controlled by content. These could have led to potential user confusion and spoofing attacks. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32205**	https://bugzilla.mozilla.org/show_bug.cgi?id=1753341, https://bugzilla.mozilla.org/show_bug.cgi?id=1753339, https://www.mozilla.org/security/advisories/mfsa2023-16/, https://www.mozilla.org/security/advisories/mfsa2023-18/	A-MOZ-THUN-280623/470
Out-of-bounds Read	02-Jun-2023	6.5	An out-of-bound read could have led to a crash in the RLBox Expat driver. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32206**	https://bugzilla.mozilla.org/show_bug.cgi?id=1824892, https://www.mozilla.org/security/advisories/mfsa2023-16/, https://www.mozilla.org/security/advisories/mfsa2023-18/, https://www.mozilla.org/security/advisories/mfsa2023-17/	A-MOZ-THUN-280623/471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	02-Jun-2023	6.5	A missing delay in popup notifications could have made it possible for an attacker to trick a user into granting permissions. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32207**	https://www.mozilla.org/security/advisories/mfsa2023-16/, https://bugzilla.mozilla.org/show_bug.cgi?id=1826116, https://www.mozilla.org/security/advisories/mfsa2023-18/, https://www.mozilla.org/security/advisories/mfsa2023-17/	A-MOZ-THUN-280623/472
N/A	02-Jun-2023	6.5	A type checking bug would have led to invalid code being compiled. This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32211**	https://www.mozilla.org/security/advisories/mfsa2023-16/, https://www.mozilla.org/security/advisories/mfsa2023-18/, https://bugzilla.mozilla.org/show_bug.cgi?id=1823379, https://www.mozilla.org/security/advisories/mfsa2023-17/	A-MOZ-THUN-280623/473
N/A	02-Jun-2023	4.3	An attacker could have positioned a <code>datalist</code> element to obscure the address bar. This	https://www.mozilla.org/security/advisories/mfsa2023-16/,	A-MOZ-THUN-280623/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11. **CVE ID : CVE-2023-32212**	https://bugzilla.mozilla.org/show_bug.cgi?id=1826622, https://www.mozilla.org/security/advisories/mfsa2023-18/, https://www.mozilla.org/security/advisories/mfsa2023-17/	
Affected Version(s): * Up to (excluding) 102.7					
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 108 and Firefox ESR 102.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 109, Thunderbird < 102.7, and Firefox ESR < 102.7. **CVE ID : CVE-2023-23605**	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://www.mozilla.org/security/advisories/mfsa2023-03/, https://www.mozilla.org/security/advisories/mfsa2023-02/	A-MOZ-THUN-280623/475
N/A	02-Jun-2023	6.5	Due to the Firefox GTK wrapper code's use of text/plain for drag data and GTK treating all text/plain MIMEs containing file URLs as	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://www.	A-MOZ-THUN-280623/476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			being dragged a website could arbitrarily read a file via a call to <code>DataTransfer.setData</code>. This vulnerability affects Firefox < 109, Thunderbird < 102.7, and Firefox ESR < 102.7. **CVE ID : CVE-2023-23598**	mozilla.org/security/advisories/mfsa2023-03/, https://www.mozilla.org/security/advisories/mfsa2023-02/, https://bugzilla.mozilla.org/show_bug.cgi?id=1800425	
Improper Encoding or Escaping of Output	02-Jun-2023	6.5	When copying a network request from the developer tools panel as a curl command the output was not being properly sanitized and could allow arbitrary commands to be hidden within. This vulnerability affects Firefox < 109, Thunderbird < 102.7, and Firefox ESR < 102.7. **CVE ID : CVE-2023-23599**	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://www.mozilla.org/security/advisories/mfsa2023-03/, https://www.mozilla.org/security/advisories/mfsa2023-02/, https://bugzilla.mozilla.org/show_bug.cgi?id=1777800	A-MOZ-THUN-280623/477
Origin Validation Error	02-Jun-2023	6.5	Navigations were being allowed when dragging a URL from a cross-origin iframe into the same tab which could lead to website spoofing attacks. This vulnerability affects Firefox < 109, Thunderbird < 102.7,	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://www.mozilla.org/security/advisories/mfsa2023-03/, https://bugzil	A-MOZ-THUN-280623/478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Firefox ESR < 102.7. **CVE ID : CVE-2023-23601**	la.mozilla.org/show_bug.cgi?id=1794268, https://www.mozilla.org/security/advisories/mfsa2023-02/	
Improper Check for Unusual or Exceptional Conditions	02-Jun-2023	6.5	A mishandled security check when creating a WebSocket in a WebWorker caused the Content Security Policy connect-src header to be ignored. This could lead to connections to restricted origins from inside WebWorkers. This vulnerability affects Firefox < 109, Thunderbird < 102.7, and Firefox ESR < 102.7. **CVE ID : CVE-2023-23602**	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://www.mozilla.org/security/advisories/mfsa2023-03/, https://www.mozilla.org/security/advisories/mfsa2023-02/, https://bugzilla.mozilla.org/show_bug.cgi?id=1800890	A-MOZ-THUN-280623/479
N/A	02-Jun-2023	6.5	Regular expressions used to filter out forbidden properties and values from style directives in calls to <code>console.log</code> weren't accounting for external URLs. Data could then be potentially exfiltrated from the browser. This vulnerability affects Firefox < 109, Thunderbird < 102.7,	https://www.mozilla.org/security/advisories/mfsa2023-01/, https://www.mozilla.org/security/advisories/mfsa2023-03/, https://www.mozilla.org/security/advisories/mfsa2023-02/, https://bugzil	A-MOZ-THUN-280623/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Firefox ESR < 102.7. **CVE ID : CVE-2023-23603**	la.mozilla.org/show_bug.cgi?id=1800832	
Affected Version(s): * Up to (excluding) 102.8					
N/A	02-Jun-2023	8.8	An attacker could construct a PKCS 12 cert bundle in such a way that could allow for arbitrary memory writes via PKCS 12 Safe Bag attributes being mishandled. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-0767**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://bugzilla.mozilla.org/show_bug.cgi?id=1804640, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-THUN-280623/481
N/A	02-Jun-2023	8.8	Permission prompts for opening external schemes were only shown for <code>ContentPrincipals</code> resulting in extensions being able to open them without user interaction via <code>ExpandedPrincipals</code>. This could lead to further malicious actions such as downloading files or interacting with software already installed on the system. This	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-THUN-280623/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25729**		
Out-of-bounds Write	02-Jun-2023	8.8	When encoding data from an <code>inputStream</code> in <code>xpcom</code> the size of the input being encoded was not correctly calculated potentially leading to an out of bounds memory write. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25732**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-THUN-280623/483
Use After Free	02-Jun-2023	8.8	Cross-compartment wrappers wrapping a scripted proxy could have caused objects from other compartments to be stored in the main compartment resulting in a use-after-free after unwrapping the proxy. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8.	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-THUN-280623/484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25735		
N/A	02-Jun-2023	8.8	An invalid downcast from <code>nsTextNode</code> to <code>SVGElement</code> could have lead to undefined behavior. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25737**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-THUN-280623/485
Use After Free	02-Jun-2023	8.8	Module load requests that failed were not being checked as to whether or not they were cancelled causing a use-after-free in <code>ScriptLoadContext</code>. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25739**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-THUN-280623/486
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers Philipp and Gabriele Svelto reported memory safety bugs present in Firefox ESR 102.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort	https://bugzilla.mozilla.org/buglist.cgi?bug_id=1544127%2C1762368, https://www.mozilla.org/security/advisories/mfsa202	A-MOZ-THUN-280623/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 102.8 and Firefox ESR < 102.8. **CVE ID : CVE-2023-25746**	3-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	
N/A	02-Jun-2023	8.1	After downloading a Windows <code>.url</code> shortcut from the local filesystem, an attacker could supply a remote path that would lead to unexpected network requests from the operating system. This also had the potential to leak NTLM credentials to the resource. *This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25734**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/, https://bugzilla.mozilla.org/show_bug.cgi?id=1784451	A-MOZ-THUN-280623/488
Uncontrolled Resource Consumption	02-Jun-2023	6.5	If a MIME email combines OpenPGP and OpenPGP MIME data in a certain way Thunderbird repeatedly attempts to process and display	https://bugzilla.mozilla.org/show_bug.cgi?id=1806507, https://www.mozilla.org/security/adviso	A-MOZ-THUN-280623/489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the message, which could cause Thunderbird's user interface to lock up and no longer respond to the user's actions. An attacker could send a crafted message with this structure to attempt a DoS attack. This vulnerability affects Thunderbird < 102.8. **CVE ID : CVE-2023-0616**	ries/mfsa2023-07/	
N/A	02-Jun-2023	6.5	The <code>Content-Security-Policy-Report-Only</code> header could allow an attacker to leak a child iframe's unredacted URI when interaction with that iframe triggers a redirect. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25728**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-THUN-280623/490
Out-of-bounds Read	02-Jun-2023	6.5	Members of the <code>DEVMODEW</code> struct set by the printer device driver weren't being validated and could have resulted in invalid values which in turn would cause the browser to attempt out of bounds access to related	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/se	A-MOZ-THUN-280623/491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variables. *This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25738**	curity/advisories/mfsa2023-06/	
N/A	02-Jun-2023	6.5	When importing a SPKI RSA public key as ECDSA P-256, the key would be handled incorrectly causing the tab to crash. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25742**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	A-MOZ-THUN-280623/492
N/A	02-Jun-2023	5.4	A background script invoking <code>requestFullscreen</code> and then blocking the main thread could force the browser into fullscreen mode indefinitely, resulting in potential user confusion or spoofing attacks. This vulnerability affects Firefox < 110, Thunderbird < 102.8,	https://bugzilla.mozilla.org/show_bug.cgi?id=1794622, https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.	A-MOZ-THUN-280623/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Firefox ESR < 102.8. **CVE ID : CVE-2023-25730**	mozilla.org/security/advisories/mfsa2023-06/	
Affected Version(s): * Up to (excluding) 102.9					
Incorrect Type Conversion or Cast	02-Jun-2023	8.8	While implementing AudioWorklets, some code may have casted one type to another, invalid, dynamic type. This could have led to a potentially exploitable crash. This vulnerability affects Firefox < 111, Firefox ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-28162**	https://www.mozilla.org/security/advisories/mfsa2023-11/, https://www.mozilla.org/security/advisories/mfsa2023-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/, https://bugzilla.mozilla.org/show_bug.cgi?id=1811327	A-MOZ-THUN-280623/494
Out-of-bounds Write	02-Jun-2023	8.8	Mozilla developers Timothy Nikkel, Andrew McCreight, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 110 and Firefox ESR 102.8. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 111,	https://www.mozilla.org/security/advisories/mfsa2023-11/, https://www.mozilla.org/security/advisories/mfsa2023-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/	A-MOZ-THUN-280623/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-28176**		
N/A	02-Jun-2023	6.5	Sometimes, when invalidating JIT code while following an iterator, the newly generated code could be overwritten incorrectly. This could lead to a potentially exploitable crash. This vulnerability affects Firefox < 111, Firefox ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-25751**	https://www.mozilla.org/security/advisories/mfsa2023-11/, https://www.mozilla.org/security/advisories/mfsa2023-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/, https://bugzilla.mozilla.org/show_bug.cgi?id=1814899	A-MOZ-THUN-280623/496
N/A	02-Jun-2023	6.5	When accessing throttled streams, the count of available bytes needed to be checked in the calling function to be within bounds. This may have lead future code to be incorrect and vulnerable. This vulnerability affects Firefox < 111, Firefox ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-25752**	https://www.mozilla.org/security/advisories/mfsa2023-11/, https://bugzilla.mozilla.org/show_bug.cgi?id=1811627, https://www.mozilla.org/security/advisories/mfsa2023-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/	A-MOZ-THUN-280623/497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jun-2023	6.5	When downloading files through the Save As dialog on Windows with suggested filenames containing environment variable names, Windows would have resolved those in the context of the current user. *This bug only affects Firefox on Windows. Other versions of Firefox are unaffected.*. This vulnerability affects Firefox < 111, Firefox ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-28163**	https://www.mozilla.org/security/advisories/mfsa2023-11/, https://bugzilla.mozilla.org/show_bug.cgi?id=1817768, https://www.mozilla.org/security/advisories/mfsa2023-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/	A-MOZ-THUN-280623/498
N/A	02-Jun-2023	6.5	Dragging a URL from a cross-origin iframe that was removed during the drag could have led to user confusion and website spoofing attacks. This vulnerability affects Firefox < 111, Firefox ESR < 102.9, and Thunderbird < 102.9. **CVE ID : CVE-2023-28164**	https://www.mozilla.org/security/advisories/mfsa2023-11/, https://bugzilla.mozilla.org/show_bug.cgi?id=1809122, https://www.mozilla.org/security/advisories/mfsa2023-10/, https://www.mozilla.org/security/advisories/mfsa2023-09/	A-MOZ-THUN-280623/499
Affected Version(s): From (including) 68.0 Up to (excluding) 102.10					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	02-Jun-2023	6.5	OCSP revocation status of recipient certificates was not checked when sending S/Mime encrypted email, and revoked certificates would be accepted. Thunderbird versions from 68 to 102.9.1 were affected by this bug. This vulnerability affects Thunderbird < 102.10. **CVE ID : CVE-2023-0547**	https://bugzilla.mozilla.org/show_bug.cgi?id=1811298, https://www.mozilla.org/security/advisories/mfsa2023-15/	A-MOZ-THUN-280623/500
Affected Version(s): From (including) 68.0 Up to (excluding) 102.7.1					
Improper Certificate Validation	02-Jun-2023	6.5	Certificate OCSP revocation status was not checked when verifying S/Mime signatures. Mail signed with a revoked certificate would be displayed as having a valid signature. Thunderbird versions from 68 to 102.7.0 were affected by this bug. This vulnerability affects Thunderbird < 102.7.1. **CVE ID : CVE-2023-0430**	https://www.mozilla.org/security/advisories/mfsa2023-04/, https://bugzilla.mozilla.org/show_bug.cgi?id=1769000	A-MOZ-THUN-280623/501
Vendor: mp4v2					
Product: mp4v2					
Affected Version(s): 2.1.3					
Missing Release of Memory after	01-Jun-2023	5.5	mp4v2 v2.1.3 was discovered to contain a memory leak via the class	https://github.com/enzo1982/mp4v2/issues/36	A-MP4-MP4V-280623/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			MP4StringProperty at mp4property.cpp. **CVE ID : CVE-2023-33716**		
Missing Release of Memory after Effective Lifetime	01-Jun-2023	5.5	mp4v2 v2.1.3 was discovered to contain a memory leak via MP4SdpAtom::Read() at atom_sdp.cpp **CVE ID : CVE-2023-33719**	https://github.com/enzo1982/mp4v2/issues/37	A-MP4-MP4V-280623/503
Vendor: mp4v2_project					
Product: mp4v2					
Affected Version(s): 2.1.3					
Missing Release of Memory after Effective Lifetime	02-Jun-2023	5.5	mp4v2 v2.1.3 was discovered to contain a memory leak when a method calling MP4File::ReadBytes() had allocated memory but did not catch exceptions thrown by ReadBytes() **CVE ID : CVE-2023-33717**	N/A	A-MP4-MP4V-280623/504
Vendor: mqtt					
Product: mqtt					
Affected Version(s): 201808021036					
Improper Authentication	01-Jun-2023	9.8	Insufficient authentication in the MQTT backend (broker) allows an attacker to access and even manipulate the telemetry data of the entire fleet of vehicles using the HopeChart HQT-401 telematics unit. Other models are possibly affected too.	N/A	A-MQT-MQTT-280623/505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Multiple vulnerabilities were identified: - The MQTT backend does not require authentication, allowing unauthorized connections from an attacker. - The vehicles publish their telemetry data (e.g. GPS Location, speed, odometer, fuel, etc) as messages in public topics. The backend also sends commands to the vehicles as MQTT posts in public topics. As a result, an attacker can access the confidential data of the entire fleet that is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			managed by the backend. - The MQTT messages sent by the vehicles or the backend are not encrypted or authenticated. An attacker can create and post messages to impersonate a vehicle or the backend. The attacker could then, for example, send incorrect information to the backend about the vehicle's location. - The backend can inject data into a vehicle´s CAN bus by sending a specific MQTT message on a public topic. Because these messages are not authenticated or encrypted, an attacker could impersonate the backend, create a fake message and inject CAN data in any vehicle managed by the backend.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The confirmed version is 201808021036, however further versions have been also identified as potentially impacted. **CVE ID : CVE-2023-3028**		
Vendor: nirmata					
Product: kyverno					
Affected Version(s): * Up to (excluding) 1.10.0					
N/A	01-Jun-2023	6.5	Kyverno is a policy engine designed for Kubernetes. In versions of Kyverno prior to 1.10.0, resources which have the `deletionTimestamp` field defined can bypass validate, generate, or mutate-existing policies, even in cases where the `validationFailureAction` field is set to `Enforce`. This situation occurs as resources pending deletion were being consciously exempted by Kyverno, as a way to reduce processing load as policies are typically not applied to objects which are being deleted.	https://github.com/kyverno/kyverno/security/advisories/GHSA-hq4m-4948-64cc	A-NIR-KYVE-280623/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			However, this could potentially result in allowing a malicious user to leverage the Kubernetes finalizers feature by setting a finalizer which causes the Kubernetes API server to set the `deletionTimestamp` and then not completing the delete operation as a way to explicitly to bypass a Kyverno policy. Note that this is not applicable to Kubernetes Pods but, as an example, a Kubernetes Service resource can be manipulated using an indefinite finalizer to bypass policies. This is resolved in Kyverno 1.10.0. There is no known workaround. **CVE ID : CVE-2023-34091**		
Vendor: niteothemes					
Product: cmp					
Affected Version(s): * Up to (excluding) 4.1.8					
Improper Access Control	09-Jun-2023	5.3	The CMP – Coming Soon & Maintenance plugin for WordPress is vulnerable to Maintenance Mode Bypass in versions up to, and including, 4.1.7. A correct cmp_bypass GET parameter in the URL	https://plugins.trac.wordpress.org/changeset/2900571/cmp-coming-soon-maintenance/tags/4.1.8/cmp-advanced.php	A-NIT-CMP-280623/507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(equal to the md5-hashed home_url in the default setting) allows users to visit a site placed in maintenance mode thus bypassing the plugin's provided feature. **CVE ID : CVE-2023-2159**	?old=2873620&old_path=cmp-coming-soon-maintenance%2Ftags%2F4.1.7%2Fcmp-advanced.php	
Vendor: notaryproject					
Product: notation					
Affected Version(s): 1.0.0					
Improper Verification of Cryptographic Signature	06-Jun-2023	8.8	notation is a CLI tool to sign and verify OCI artifacts and container images. An attacker who has compromised a registry can cause users to verify the wrong artifact. The problem has been fixed in the release v1.0.0-rc.6. Users should upgrade their notation-go library to v1.0.0-rc.6 or above. Users unable to upgrade may restrict container registries to a set of secure and trusted container registries. **CVE ID : CVE-2023-33959**	https://github.com/notaryproject/notation-go/security/advisories/GHSA-xhg5-42rf-296r	A-NOT-NOTA-280623/508
Uncontrolled Resource Consumption	06-Jun-2023	6.5	notation is a CLI tool to sign and verify OCI artifacts and container images. An attacker who has compromised a registry and added a	https://github.com/notaryproject/notation/security/advisories/GH	A-NOT-NOTA-280623/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			high number of signatures to an artifact can cause denial of service of services on the machine, if a user runs notation verify command on the same machine. The problem has been fixed in the release v1.0.0-rc.6. Users should upgrade their notation packages to v1.0.0-rc.6 or above. Users unable to upgrade may restrict container registries to a set of secure and trusted container registries. **CVE ID : CVE-2023-33958**	SA-rvrx-rrwh-r9p6	
Uncontrolled Resource Consumption	06-Jun-2023	5.7	notation is a CLI tool to sign and verify OCI artifacts and container images. An attacker who has compromised a registry and added a high number of signatures to an artifact can cause denial of service of services on the machine, if a user runs notation inspect command on the same machine. The problem has been fixed in the release v1.0.0-rc.6. Users should upgrade their notation packages to v1.0.0-rc.6 or above. Users	https://github.com/notaryproject/notation/security/advisories/GHSA-9m3v-v4r5-ppx7, https://github.com/notaryproject/notation/commit/ed22fde52f6d70ae0b53521bd28c9ccafa868c24	A-NOT-NOTA-280623/510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are advised to upgrade. Users unable to upgrade may restrict container registries to a set of secure and trusted container registries. **CVE ID : CVE-2023-33957**		
Affected Version(s): * Up to (excluding) 1.0.0					
Improper Verification of Cryptographic Signature	06-Jun-2023	8.8	notation is a CLI tool to sign and verify OCI artifacts and container images. An attacker who has compromised a registry can cause users to verify the wrong artifact. The problem has been fixed in the release v1.0.0-rc.6. Users should upgrade their notation-go library to v1.0.0-rc.6 or above. Users unable to upgrade may restrict container registries to a set of secure and trusted container registries. **CVE ID : CVE-2023-33959**	https://github.com/notaryproject/notation-go/security/advisories/GHSA-xhg5-42rf-296r	A-NOT-NOTA-280623/511
Uncontrolled Resource Consumption	06-Jun-2023	6.5	notation is a CLI tool to sign and verify OCI artifacts and container images. An attacker who has compromised a registry and added a high number of signatures to an artifact can cause denial of service of	https://github.com/notaryproject/notation/security/advisories/GHSA-rvrx-rrwh-r9p6	A-NOT-NOTA-280623/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			services on the machine, if a user runs notation verify command on the same machine. The problem has been fixed in the release v1.0.0-rc.6. Users should upgrade their notation packages to v1.0.0-rc.6 or above. Users unable to upgrade may restrict container registries to a set of secure and trusted container registries. **CVE ID : CVE-2023-33958**		
Uncontrolled Resource Consumption	06-Jun-2023	5.7	notation is a CLI tool to sign and verify OCI artifacts and container images. An attacker who has compromised a registry and added a high number of signatures to an artifact can cause denial of service of services on the machine, if a user runs notation inspect command on the same machine. The problem has been fixed in the release v1.0.0-rc.6. Users should upgrade their notation packages to v1.0.0-rc.6 or above. Users are advised to upgrade. Users unable to upgrade may restrict container	https://github.com/notaryproject/notation/security/advisories/GHSA-9m3v-v4r5-ppx7, https://github.com/notaryproject/notation/commit/ed22fde52f6d70ae0b53521bd28c9ccafa868c24	A-NOT-NOTA-280623/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			registries to a set of secure and trusted container registries. **CVE ID : CVE-2023-33957**		
Vendor: nsqua					
Product: draw_attention					
Affected Version(s): * Up to (including) 2.0.11					
Missing Authorization	09-Jun-2023	4.3	The Draw Attention plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ajax_set_featured_image function in versions up to, and including, 2.0.11. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to change the featured image of arbitrary posts with an image that exists in the media library. **CVE ID : CVE-2023-2764**	https://plugins.trac.wordpress.org/browser/draw-attention/trunk/public/includes/lib/drag-drop-featured-image/index.php#L500, https://plugins.trac.wordpress.org/changeset/2917528/	A-NSQ-DRAW-280623/514
Vendor: online_discussion_forum_site_project					
Product: online_discussion_forum_site					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an	07-Jun-2023	8.8	A vulnerability, which was classified as critical, has been found in SourceCodester Online Discussion	N/A	A-ONL-ONLI-280623/515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			Forum Site 1.0. Affected by this issue is some unknown functionality of the file classes\Users.php?f=registration. The manipulation of the argument username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-231014 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3145**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jun-2023	8.8	A vulnerability, which was classified as critical, was found in SourceCodester Online Discussion Forum Site 1.0. This affects an unknown part of the file admin\categories\manage_category.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-231015. **CVE ID : CVE-2023-3146**	N/A	A-ONL-ONLI-280623/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jun-2023	8.8	A vulnerability has been found in SourceCodester Online Discussion Forum Site 1.0 and classified as critical. This vulnerability affects unknown code of the file admin\categories\view_category.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-231016. **CVE ID : CVE-2023-3147**	N/A	A-ONL-ONLI-280623/517
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jun-2023	8.8	A vulnerability was found in SourceCodester Online Discussion Forum Site 1.0 and classified as critical. This issue affects some unknown processing of the file admin\posts\manage_post.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-231017	N/A	A-ONL-ONLI-280623/518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was assigned to this vulnerability. **CVE ID : CVE-2023-3148**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jun-2023	8.8	A vulnerability was found in SourceCodester Online Discussion Forum Site 1.0. It has been classified as critical. Affected is an unknown function of the file admin\user\manage_user.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-231018 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3149**	N/A	A-ONL-ONLI-280623/519
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jun-2023	8.8	A vulnerability was found in SourceCodester Online Discussion Forum Site 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file posts\manage_post.php. The manipulation of the argument id leads to sql injection. The attack can be launched	N/A	A-ONL-ONLI-280623/520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-231019. **CVE ID : CVE-2023-3150**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jun-2023	8.8	A vulnerability was found in SourceCodester Online Discussion Forum Site 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file user\manage_user.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-231020. **CVE ID : CVE-2023-3151**	N/A	A-ONL-ONLI-280623/521
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jun-2023	8.8	A vulnerability classified as critical has been found in SourceCodester Online Discussion Forum Site 1.0. This affects an unknown part of the file admin\posts\view_post.php. The manipulation leads to	N/A	A-ONL-ONLI-280623/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-231021 was assigned to this vulnerability. **CVE ID : CVE-2023-3152**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2023	5.4	A vulnerability classified as problematic has been found in SourceCodester Online Discussion Forum Site 1.0. Affected is an unknown function of the file admin\posts\manage_post.php. The manipulation of the argument content leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-231012. **CVE ID : CVE-2023-3143**	N/A	A-ONL-ONLI-280623/523
Improper Neutralization of Input During Web Page Generation	07-Jun-2023	5.4	A vulnerability classified as problematic was found in SourceCodester Online Discussion Forum Site 1.0.	N/A	A-ONL-ONLI-280623/524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Affected by this vulnerability is an unknown functionality of the file admin\posts\manage_post.php. The manipulation of the argument title leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-231013 was assigned to this vulnerability. **CVE ID : CVE-2023-3144**		
Vendor: online_exam_form_submission_project					
Product: online_exam_form_submission					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Online Exam Form Submission 1.0. This affects an unknown part of the file /admin/update_s6.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-230565 was assigned to this vulnerability.	N/A	A-ONL-ONLI-280623/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3059		
Vendor: ooohboi_steroids_for_elementor_project					
Product: ooohboi_steroids_for_elementor					
Affected Version(s): * Up to (including) 2.1.4					
Missing Authorization	09-Jun-2023	4.3	The OoohBoi Steroids for Elementor plugin for WordPress is vulnerable to missing authorization due to a missing capability check on the 'file_uploader_callback' function in versions up to, and including, 2.1.4. This makes it possible for subscriber-level attackers to upload image attachments to the site. **CVE ID : CVE-2023-1169**	https://plugins.trac.wordpress.org/browser/ooohboi-steroids-for-elementor/tags/2.1.3/inc/exopite-simple-options/upload-class.php	A-OOO-OOOH-280623/526
Vendor: openfind					
Product: mail2000					
Affected Version(s): * Up to (excluding) 8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-2023	6.1	Openfind Mail2000 has insufficient filtering special characters of email content of its content filtering function. A remote attacker can exploit this vulnerability using phishing emails that contain malicious web pages injected with JavaScript. When users access the system and open the	N/A	A-OPE-MAIL-280623/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			email, it triggers an XSS (Reflected Cross-site scripting) attack. **CVE ID : CVE-2023-28705**		
Vendor: openprinting					
Product: cups					
Affected Version(s): * Up to (including) 2.4.2					
Out-of-bounds Write	01-Jun-2023	5.5	OpenPrinting CUPS is an open source printing system. In versions 2.4.2 and prior, a heap buffer overflow vulnerability would allow a remote attacker to launch a denial of service (DoS) attack. A buffer overflow vulnerability in the function `format_log_line` could allow remote attackers to cause a DoS on the affected system. Exploitation of the vulnerability can be triggered when the configuration file `cupsd.conf` sets the value of `loglevel `to `DEBUG`. No known patches or workarounds exist at time of publication. **CVE ID : CVE-2023-32324**	https://github.com/OpenPrinting/cups/security/advisories/GHSA-cxc6-w2g7-69p7	A-OPE-CUPS-280623/528
Vendor: openproject					
Product: openproject					
Affected Version(s): * Up to (excluding) 12.5.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	01-Jun-2023	7.5	OpenProject is web-based project management software. For any OpenProject installation, a `robots.txt` file is generated through the server to denote which routes shall or shall not be accessed by crawlers. These routes contain project identifiers of all public projects in the instance. Prior to version 12.5.6, even if the entire instance is marked as `Login required` and prevents all truly anonymous access, the `/robots.txt` route remains publicly available. Version 12.5.6 has a fix for this issue. Alternatively, users can download a patchfile to apply the patch to any OpenProject version greater than 10.0 As a workaround, one may mark any public project as non-public and give anyone in need of access to the project a membership. **CVE ID : CVE-2023-33960**	https://github.com/opf/openproject/security/advisories/GHSA-xjfc-fqm3-95q8, https://patch-diff.githubusercontent.com/raw/opf/openproject/pull/12708.patch, https://github.com/opf/openproject/pull/12708	A-OPE-OPEN-280623/529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: opensc_project					
Product: opensc					
Affected Version(s): 0.23.0					
Out-of-bounds Read	01-Jun-2023	7.1	A vulnerbility was found in OpenSC. This security flaw cause a buffer overrun vulnerability in pkcs15 cardos_have_verifyrc_package. The attacker can supply a smart card package with malformed ASN1 context. The cardos_have_verifyrc_package function scans the ASN1 buffer for 2 tags, where remaining length is wrongly caculated due to moved starting pointer. This leads to possible heap-based buffer oob read. In cases where ASAN is enabled while compiling this causes a crash. Further info leak or more damage is possible. **CVE ID : CVE-2023-2977**	https://github.com/OpenSC/OpenSC/issues/2785, https://github.com/OpenSC/OpenSC/pull/2787	A-OPE-OPEN-280623/530
Vendor: Opensuse					
Product: libeconf					
Affected Version(s): * Up to (excluding) 0.5.2					
Buffer Copy without Checking Size of	01-Jun-2023	6.5	A Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in	https://bugzilla.suse.com/show_bug.cgi?id=CVE-2023-22652	A-OPE-LIBE-280623/531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			openSUSE libeconf leads to DoS via malformed config files. This issue affects libeconf: before 0.5.2. **CVE ID : CVE-2023-22652**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jun-2023	6.5	A Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in openSUSE libeconf allows for DoS via malformed configuration files This issue affects libeconf: before 0.5.2. **CVE ID : CVE-2023-32181**	https://https://bugzilla.suse.com/show_bug.cgi?id=CVE-2023-32181, https://https://github.com/openSUSE/libeconf/issues/178	A-OPE-LIBE-280623/532
Vendor: openzeppelin					
Product: contracts					
Affected Version(s): From (including) 4.3.0 Up to (excluding) 4.9.1					
N/A	07-Jun-2023	5.3	OpenZeppelin Contracts is a library for smart contract development. By frontrunning the creation of a proposal, an attacker can become the proposer and gain the ability to cancel it. The attacker can do this repeatedly to try to prevent a proposal from being	https://github.com/OpenZeppelin/openzeppelin-contracts/commit/d9474327a492f9f310f31bc53f38dbea56ed9a57, https://github.com/OpenZeppelin/openzeppelin-	A-OPE-CONT-280623/533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			proposed at all. This impacts the `Governor` contract in v4.9.0 only, and the `GovernorCompatibilityBravo` contract since v4.3.0. This problem has been patched in 4.9.1 by introducing opt-in frontrunning protection. Users are advised to upgrade. Users unable to upgrade may submit the proposal creation transaction to an endpoint with frontrunning protection as a workaround. **CVE ID : CVE-2023-34234**	contracts/security/advisories/GHSA-5h3x-9wvq-w4m2	
Product: contracts_upgradeable					
Affected Version(s): From (including) 4.3.0 Up to (excluding) 4.9.1					
N/A	07-Jun-2023	5.3	OpenZeppelin Contracts is a library for smart contract development. By frontrunning the creation of a proposal, an attacker can become the proposer and gain the ability to cancel it. The attacker can do this repeatedly to try to prevent a proposal from being proposed at all. This impacts the `Governor` contract in v4.9.0 only, and the `GovernorCompatibilityBravo` contract since	https://github.com/OpenZeppelin/openzeppelin-contracts/commit/d9474327a492f9f310f31bc53f38dbea56ed9a57, https://github.com/OpenZeppelin/openzeppelin-contracts/security/advisories/GHSA-5h3x-9wvq-w4m2	A-OPE-CONT-280623/534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.3.0. This problem has been patched in 4.9.1 by introducing opt-in frontrunning protection. Users are advised to upgrade. Users unable to upgrade may submit the proposal creation transaction to an endpoint with frontrunning protection as a workaround. **CVE ID : CVE-2023-34234**		
Vendor: owncast_project					
Product: owncast					
Affected Version(s): * Up to (excluding) 0.1.0					
Server-Side Request Forgery (SSRF)	10-Jun-2023	6.5	Server-Side Request Forgery (SSRF) in GitHub repository owncast/owncast prior to 0.1.0. **CVE ID : CVE-2023-3188**	https://huntr.dev/bounties/0d0d526a-1c39-4e6a-b081-d3914468e495, https://github.com/owncast/owncast/commit/f40135dbf2809386482f9662c23e478ea192b16	A-OWN-OWNC-280623/535
Vendor: palantir					
Product: foundry_comments					
Affected Version(s): * Up to (excluding) 2.249.0					
Missing Authorization	06-Jun-2023	6.5	A security defect in Foundry's Comments functionality resulted in the retrieval of	https://palantir.safebase.us/?tcuUid=101b083b-6389-	A-PAL-FOUN-280623/536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attachments to comments not being gated by additional authorization checks. This could enable an authenticated user to inject a prior discovered attachment UUID into other arbitrary comments to discover it's content. This defect was fixed in Foundry Comments 2.249.0, and a patch was rolled out to affected Foundry environments. No further intervention is required at this time. **CVE ID : CVE-2023-30948**	4261-98f8-23448e133a62	
Vendor: pega					
Product: pega_platform					
Affected Version(s): From (including) 7.2 Up to (including) 8.8.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	6.1	Pega Platform versions 7.2 to 8.8.1 are affected by an XSS issue. **CVE ID : CVE-2023-26465**	https://support.pega.com/support-doc/pega-security-advisory-a23-vulnerability-remediation-note	A-PEG-PEGA-280623/537
Vendor: performance_indicator_system_project					
Product: performance_indicator_system					
Affected Version(s): 1.0					
Improper Neutralizat	09-Jun-2023	5.4	A vulnerability was found in	N/A	A-PER-PERF-280623/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			SourceCodester Performance Indicator System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/addproduct.php. The manipulation of the argument prodname 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-231163. **CVE ID : CVE-2023-3183**		
Vendor: phpok					
Product: phpok					
Affected Version(s): 6.4.100					
Unrestricted Upload of File with Dangerous Type	07-Jun-2023	8.8	An arbitrary file upload vulnerability in /admin.php?c=upload of phpok v6.4.100 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2023-33601**	N/A	A-PHP-PHPO-280623/539
Vendor: pixelyoursite					
Product: pixelyoursite					
Affected Version(s): * Up to (including) 9.3.6					
Improper Neutralization of	09-Jun-2023	4.8	The PixelYourSite plugin for WordPress is vulnerable to Stored	https://plugins.trac.wordpress.org/brows	A-PIX-PIXE-280623/540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Cross-Site Scripting via admin settings in versions up to, and including, 9.3.6 (9.6.1 in the Pro version) due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-2584**	er/pixelyoursite/trunk/modules/head_footer/head_footer.php?rev=2773949#L73	
Product: pixelyoursite_pro					
Affected Version(s): * Up to (including) 9.6.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	4.8	The PixelYourSite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 9.3.6 (9.6.1 in the Pro version) due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level	https://plugins.trac.wordpress.org/browser/pixelyoursite/trunk/modules/head_footer/head_footer.php?rev=2773949#L73	A-PIX-PIXE-280623/541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-2584**		
Vendor: plainware					
Product: locatoraid					
Affected Version(s): * Up to (including) 3.9.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	5.4	The Locatoraid Store Locator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in versions up to, and including, 3.9.14 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	https://plugins.trac.wordpress.org/changeset/2900106/locatoraid, https://plugins.trac.wordpress.org/browser/locatoraid/trunk/modules/front/view_shortcode.php#L4	A-PLA-LOCA-280623/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2031		
Product: shiftcontroller					
Affected Version(s): * Up to (including) 4.9.25					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	6.1	The ShiftController Employee Shift Scheduling plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the query string in versions up to, and including, 4.9.25 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2023-1978**	https://plugins.trac.wordpress.org/changeset/2898274/shiftcontroller	A-PLA-SHIF-280623/543
Vendor: pleasanter					
Product: pleasanter					
Affected Version(s): * Up to (excluding) 1.3.38.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-2023	5.4	Cross-site scripting vulnerability in Pleasanter 1.3.38.1 and earlier allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-30758**	https://github.com/Implem/Implem.Pleasanter/issues/474, https://pleasanter.org/archives/vulnerabi	A-PLE-PLEA-280623/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lity-update-202305	
Vendor: pluginus					
Product: wordpress_currency_switcher					
Affected Version(s): * Up to (excluding) 1.2.0					
Missing Authorization	09-Jun-2023	4.3	The WPCS – WordPress Currency Switcher Professional plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the anonymous function for the wpcs_sd_delete action in versions up to, and including, 1.1.9. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to delete an arbitrary custom drop-down currency switcher. **CVE ID : CVE-2023-2556**	https://plugins.trac.wordpress.org/changeset/2911049/currency-switcher	A-PLU-WORD-280623/545
Product: wordpress_currency_switcher_professional					
Affected Version(s): * Up to (including) 1.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	5.4	The WPCS – WordPress Currency Switcher Professional plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wpcs_current_currency shortcode in	https://plugins.trac.wordpress.org/changeset/2911049/currency-switcher	A-PLU-WORD-280623/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions up to, and including, 1.1.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-2558**		
Missing Authorization	09-Jun-2023	4.3	The WPCS – WordPress Currency Switcher Professional plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the create function in versions up to, and including, 1.1.9. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to create a custom drop-down currency switcher. **CVE ID : CVE-2023-2555**	https://plugins.trac.wordpress.org/changeset/2911049/currency-switcher	A-PLU-WORD-280623/547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	09-Jun-2023	4.3	The WPCS – WordPress Currency Switcher Professional plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save function in versions up to, and including, 1.1.9. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to edit an arbitrary custom drop-down currency switcher. **CVE ID : CVE-2023-2557**	https://plugins.trac.wordpress.org/changeset/2911049/currency-switcher	A-PLU-WORD-280623/548
Vendor: Prestashop					
Product: prestashop					
Affected Version(s): 1.5.0.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	SQL injection vulnerability in the City Autocomplete (cityautocomplete) module from ebewe.net for PrestaShop, prior to version 1.8.12 (for PrestaShop version 1.5/1.6) or prior to 2.0.3 (for PrestaShop version 1.7), allows remote attackers to execute arbitrary SQL commands via the type, input_name. or q	N/A	A-PRE-PRES-280623/549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter in the autocompletion.php front controller. **CVE ID : CVE-2023-30149**		
Affected Version(s): 1.6.0.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	SQL injection vulnerability in the City Autocomplete (cityautocomplete) module from ebewe.net for PrestaShop, prior to version 1.8.12 (for PrestaShop version 1.5/1.6) or prior to 2.0.3 (for PrestaShop version 1.7), allows remote attackers to execute arbitrary SQL commands via the type, input_name. or q parameter in the autocompletion.php front controller. **CVE ID : CVE-2023-30149**	N/A	A-PRE-PRES-280623/550
Affected Version(s): 1.7.0.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	SQL injection vulnerability in the City Autocomplete (cityautocomplete) module from ebewe.net for PrestaShop, prior to version 1.8.12 (for PrestaShop version 1.5/1.6) or prior to 2.0.3 (for PrestaShop version 1.7), allows remote attackers to execute arbitrary SQL	N/A	A-PRE-PRES-280623/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via the type, input_name. or q parameter in the autocompletion.php front controller. **CVE ID : CVE-2023-30149**		
Vendor: Progress					
Product: moveit_cloud					
Affected Version(s): * Up to (excluding) 14.0.5.45					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database, and execute SQL statements that alter or delete database elements. NOTE: this is exploited in the wild in May and June 2023;	https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023	A-PRO-MOVE-280623/552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of unpatched systems can occur via HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions. **CVE ID : CVE-2023-34362**		
Affected Version(s): From (including) 14.1.0.0 Up to (excluding) 14.1.6.97					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database, and execute SQL statements that alter or delete database elements. NOTE: this	https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023	A-PRO-MOVE-280623/553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is exploited in the wild in May and June 2023; exploitation of unpatched systems can occur via HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions. **CVE ID : CVE-2023-34362**		
Affected Version(s): From (including) 15.0.0.0 Up to (excluding) 15.0.2.39					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database, and execute SQL statements that alter	https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023	A-PRO-MOVE-280623/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or delete database elements. NOTE: this is exploited in the wild in May and June 2023; exploitation of unpatched systems can occur via HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions. **CVE ID : CVE-2023-34362**		
Product: moveit_transfer					
Affected Version(s): * Up to (including) 2020.1.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents	https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023	A-PRO-MOVE-280623/555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the database, and execute SQL statements that alter or delete database elements. NOTE: this is exploited in the wild in May and June 2023; exploitation of unpatched systems can occur via HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions. **CVE ID : CVE-2023-34362**		
Affected Version(s): From (including) 2021.0 Up to (excluding) 2021.0.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer	https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023	A-PRO-MOVE-280623/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about the structure and contents of the database, and execute SQL statements that alter or delete database elements. NOTE: this is exploited in the wild in May and June 2023; exploitation of unpatched systems can occur via HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions. **CVE ID : CVE-2023-34362**		
Affected Version(s): From (including) 2021.1.0 Up to (excluding) 2021.1.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure	https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023	A-PRO-MOVE-280623/557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SQL), an attacker may be able to infer information about the structure and contents of the database, and execute SQL statements that alter or delete database elements. NOTE: this is exploited in the wild in May and June 2023; exploitation of unpatched systems can occur via HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions. **CVE ID : CVE-2023-34362**		
Affected Version(s): From (including) 2022.0.0 Up to (excluding) 2022.0.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. Depending on the database engine being used	https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023	A-PRO-MOVE-280623/558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database, and execute SQL statements that alter or delete database elements. NOTE: this is exploited in the wild in May and June 2023; exploitation of unpatched systems can occur via HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions. **CVE ID : CVE-2023-34362**		
Affected Version(s): From (including) 2022.1.0 Up to (excluding) 2022.1.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. Depending	https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023	A-PRO-MOVE-280623/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database, and execute SQL statements that alter or delete database elements. NOTE: this is exploited in the wild in May and June 2023; exploitation of unpatched systems can occur via HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions. **CVE ID : CVE-2023-34362**		
Affected Version(s): From (including) 2023.0.0 Up to (excluding) 2023.0.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access	https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023	A-PRO-MOVE-280623/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database, and execute SQL statements that alter or delete database elements. NOTE: this is exploited in the wild in May and June 2023; exploitation of unpatched systems can occur via HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions. **CVE ID : CVE-2023-34362**		
Vendor: promptworks					
Product: redcloth					
Affected Version(s): From (including) 4.0.0 Up to (including) 4.3.2					
N/A	06-Jun-2023	7.5	A Regular Expression Denial of Service (ReDoS) issue was discovered in the sanitize_html function of redcloth gem v4.0.0. This vulnerability allows attackers to cause a Denial of Service (DoS) via	N/A	A-PRO-REDC-280623/561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplying a crafted payload. **CVE ID : CVE-2023-31606**		
Vendor: protobuf					
Product: protobuf					
Affected Version(s): 1.29.0					
Out-of-bounds Read	08-Jun-2023	7.5	Parsing invalid messages can panic. Parsing a text-format message which contains a potential number consisting of a minus sign, one or more characters of whitespace, and no further input will cause a panic. **CVE ID : CVE-2023-24535**	https://go.dev/cl/475995	A-PRO-PROT-280623/562
Vendor: PTC					
Product: vuforia_studio					
Affected Version(s): * Up to (excluding) 9.9					
N/A	07-Jun-2023	8.1	By changing the filename parameter in the request, an attacker could delete any file with the permissions of the Vuforia server account. **CVE ID : CVE-2023-29152**	N/A	A-PTC-VUFO-280623/563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Jun-2023	4.3	Before importing a project into Vuforia, a user could modify the "resourceDirectory" attribute in the appConfig.json file to be a different path. **CVE ID : CVE-2023-29502**	N/A	A-PTC-VUFO-280623/564
N/A	07-Jun-2023	3.3	An attacker with local access to the machine could record the traffic, which could allow them to resend requests without the server authenticating that the user or session are valid. **CVE ID : CVE-2023-24476**	N/A	A-PTC-VUFO-280623/565
Vendor: punchcreative					
Product: get_your_number					
Affected Version(s): * Up to (including) 1.1.3					
Improper Neutralizat	05-Jun-2023	4.8	The Get your number WordPress plugin	N/A	A-PUN-GET_-280623/566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			through 1.1.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-2634**		
Vendor: Puppet					
Product: puppet_enterprise					
Affected Version(s): 2023.0					
N/A	07-Jun-2023	9.8	A privilege escalation allowing remote code execution was discovered in the orchestration service. **CVE ID : CVE-2023-2530**	https://www.puppet.com/security/cve/cve-2023-2530-remote-code-execution-orchestrator	A-PUP-PUPP-280623/567
Affected Version(s): 2023.1.0					
N/A	07-Jun-2023	9.8	A privilege escalation allowing remote code execution was discovered in the orchestration service. **CVE ID : CVE-2023-2530**	https://www.puppet.com/security/cve/cve-2023-2530-remote-code-execution-orchestrator	A-PUP-PUPP-280623/568
Affected Version(s): From (including) 2021.7.0 Up to (including) 2021.7.3					
N/A	07-Jun-2023	9.8	A privilege escalation allowing remote code execution was	https://www.puppet.com/security/cve/cve-2023-	A-PUP-PUPP-280623/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered in the orchestration service. **CVE ID : CVE-2023-2530**	2530-remote-code-execution-orchestrator	
Vendor: Pydio					
Product: cells					
Affected Version(s): * Up to (excluding) 3.0.12					
Incorrect Authorization	08-Jun-2023	8.8	Pydio Cells allows users by default to create so-called external users in order to share files with them. By modifying the HTTP request sent when creating such an external user, it is possible to assign the new user arbitrary roles. By assigning all roles to a newly created user, access to all cells and non-personal workspaces is granted. **CVE ID : CVE-2023-32749**	N/A	A-PYD-CELL-280623/570
Affected Version(s): From (including) 4.1.0 Up to (excluding) 4.1.3					
Incorrect Authorization	08-Jun-2023	8.8	Pydio Cells allows users by default to create so-called external users in order to share files with them. By modifying the HTTP request sent when creating such an external user, it is possible to assign the new user arbitrary roles. By assigning all	N/A	A-PYD-CELL-280623/571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			roles to a newly created user, access to all cells and non-personal workspaces is granted. **CVE ID : CVE-2023-32749**		
Vendor: pythagorean_oa_office_system_project					
Product: pythagorean_oa_office_system					
Affected Version(s): * Up to (including) 4.50.31					
Cross-Site Request Forgery (CSRF)	01-Jun-2023	8.8	A vulnerability has been found in Guangdong Pythagorean OA Office System up to 4.50.31 and classified as problematic. This vulnerability affects unknown code of the file /note/index/delete. The manipulation of the argument id leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-230458 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3029**	N/A	A-PYT-PYTH-280623/572
Vendor: Python					
Product: cpython					
Affected Version(s): 3.12.0					
Use After Free	07-Jun-2023	5.5	CPython v3.12.0 alpha 7 was discovered to contain a heap use-after-free via the	https://github.com/python/cpython/issues/103824,	A-PYT-CPYT-280623/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function ascii_decode at /Objects/unicodeobject.c. **CVE ID : CVE-2023-33595**	https://github.com/python/cpython/pull/103993/commits/c120bc2d354ca3d27d0c7a53bf65574ddaabaf3a	
Vendor: QT					
Product: qt					
Affected Version(s): * Up to (excluding) 5.15.15					
Improper Certificate Validation	05-Jun-2023	5.3	An issue was discovered in Qt before 5.15.15, 6.x before 6.2.9, and 6.3.x through 6.5.x before 6.5.2. Certificate validation for TLS does not always consider whether the root of a chain is a configured CA certificate. **CVE ID : CVE-2023-34410**	https://codereview.qt-project.org/c/qt/qtbase/+/477560, https://codereview.qt-project.org/c/qt/qtbase/+/480002	A-QT-QT-280623/574
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.2.9					
Improper Certificate Validation	05-Jun-2023	5.3	An issue was discovered in Qt before 5.15.15, 6.x before 6.2.9, and 6.3.x through 6.5.x before 6.5.2. Certificate validation for TLS does not always consider whether the root of a chain is a configured CA certificate. **CVE ID : CVE-2023-34410**	https://codereview.qt-project.org/c/qt/qtbase/+/477560, https://codereview.qt-project.org/c/qt/qtbase/+/480002	A-QT-QT-280623/575
Affected Version(s): From (including) 6.3.0 Up to (excluding) 6.5.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	05-Jun-2023	5.3	An issue was discovered in Qt before 5.15.15, 6.x before 6.2.9, and 6.3.x through 6.5.x before 6.5.2. Certificate validation for TLS does not always consider whether the root of a chain is a configured CA certificate. **CVE ID : CVE-2023-34410**	https://codereview.qt-project.org/c/qt/qtbase/+/477560, https://codereview.qt-project.org/c/qt/qtbase/+/480002	A-QT-QT-280623/576
Vendor: rdkcentral					
Product: rdk-b					
Affected Version(s): 2022q3					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	A-RDK-RDK--280623/577
Vendor: readymedia_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: readymedia					
Affected Version(s): From (including) 1.1.15 Up to (including) 1.3.2					
Out-of-bounds Write	02-Jun-2023	9.8	ReadyMedia (MiniDLNA) versions from 1.1.15 up to 1.3.2 is vulnerable to Buffer Overflow. The vulnerability is caused by incorrect validation logic when handling HTTP requests using chunked transport encoding. This results in other code later using attacker-controlled chunk values that exceed the length of the allocated buffer, resulting in out-of-bounds read/write. **CVE ID : CVE-2023-33476**	https://sourceforge.net/p/minidlna/git/ci/9bd58553fae5aef3e6dd22f51642d2c851225aec/	A-REA-READ-280623/578
Vendor: Redhat					
Product: advanced_cluster_management_for_kubernetes					
Affected Version(s): 2.5					
Improper Privilege Management	05-Jun-2023	7.8	The grc-policy-propagator allows security escalation within the cluster. The propagator allows policies which contain some dynamically obtained values (instead of the policy apply a static manifest on a managed cluster) of taking advantage of cluster scoped access in a created policy. This feature does not restrict properly to	https://bugzilla.redhat.com/show_bug.cgi?id=2211468#c0	A-RED-ADVA-280623/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lookup content from the namespace where the policy was created. **CVE ID : CVE-2023-3027**		
Affected Version(s): 2.6					
Improper Privilege Management	05-Jun-2023	7.8	The grc-policy-propagator allows security escalation within the cluster. The propagator allows policies which contain some dynamically obtained values (instead of the policy apply a static manifest on a managed cluster) of taking advantage of cluster scoped access in a created policy. This feature does not restrict properly to lookup content from the namespace where the policy was created. **CVE ID : CVE-2023-3027**	https://bugzilla.redhat.com/show_bug.cgi?id=2211468#c0	A-RED-ADVA-280623/580
Affected Version(s): 2.7					
Improper Privilege Management	05-Jun-2023	7.8	The grc-policy-propagator allows security escalation within the cluster. The propagator allows policies which contain some dynamically obtained values (instead of the policy apply a static manifest on a managed cluster) of taking advantage of cluster scoped access in a created policy.	https://bugzilla.redhat.com/show_bug.cgi?id=2211468#c0	A-RED-ADVA-280623/581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This feature does not restrict properly to lookup content from the namespace where the policy was created. **CVE ID : CVE-2023-3027**		
Product: openshift_api_for_data_protection					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	06-Jun-2023	6.5	A flaw was found in the `/v2/_catalog` endpoint in distribution/distribution, which accepts a parameter to control the maximum number of records returned (query string: `n`). This vulnerability allows a malicious user to submit an unreasonably large value for `n,` causing the allocation of a massive string array, possibly causing a denial of service through excessive use of memory. **CVE ID : CVE-2023-2253**	N/A	A-RED-OPEN-280623/582
Product: openshift_container_platform					
Affected Version(s): 4.0					
Allocation of Resources Without Limits or Throttling	06-Jun-2023	6.5	A flaw was found in the `/v2/_catalog` endpoint in distribution/distribution, which accepts a parameter to control the maximum number of records returned	N/A	A-RED-OPEN-280623/583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(query string: `n`). This vulnerability allows a malicious user to submit an unreasonably large value for `n,` causing the allocation of a massive string array, possibly causing a denial of service through excessive use of memory. **CVE ID : CVE-2023-2253**		
Product: openshift_developer_tools_and_services					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	06-Jun-2023	6.5	A flaw was found in the `/v2/_catalog` endpoint in distribution/distribution, which accepts a parameter to control the maximum number of records returned (query string: `n`). This vulnerability allows a malicious user to submit an unreasonably large value for `n,` causing the allocation of a massive string array, possibly causing a denial of service through excessive use of memory. **CVE ID : CVE-2023-2253**	N/A	A-RED-OPEN-280623/584
Vendor: renderdoc					
Product: renderdoc					
Affected Version(s): * Up to (including) 1.26					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-Jun-2023	9.8	RenderDoc through 1.26 allows an Integer Overflow with a resultant Buffer Overflow (issue 1 of 2). **CVE ID : CVE-2023-33863**	N/A	A-REN-REND-280623/585
Integer Overflow or Wraparound	07-Jun-2023	9.8	RenderDoc through 1.26 allows an Integer Overflow with a resultant Buffer Overflow (issue 2 of 2). **CVE ID : CVE-2023-33864**	N/A	A-REN-REND-280623/586
Improper Link Resolution Before File Access ('Link Following')	07-Jun-2023	7.8	RenderDoc through 1.26 allows local privilege escalation via a symlink attack. **CVE ID : CVE-2023-33865**	N/A	A-REN-REND-280623/587
Vendor: reportlab					
Product: reportlab					
Affected Version(s): * Up to (including) 3.6.12					
N/A	05-Jun-2023	7.8	Reportlab up to v3.6.12 allows attackers to execute arbitrary code via supplying a crafted PDF file. **CVE ID : CVE-2023-33733**	N/A	A-REP-REPO-280623/588
Vendor: retro_cellphone_online_store_project					
Product: retro_cellphone_online_store					
Affected Version(s): 1.0					
Improper Neutralizat	02-Jun-2023	9.8	A vulnerability classified as critical	N/A	A-RET-RETR-280623/589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			has been found in Campcodes Retro Cellphone Online Store 1.0. Affected is an unknown function of the file /admin/modal_add_product.php. The manipulation of the argument category 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-230580. **CVE ID : CVE-2023-3068**		
Vendor: ruoyi					
Product: ruoyi					
Affected Version(s): * Up to (including) 4.7.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jun-2023	7.5	A vulnerability was found in y_project RuoYi up to 4.7.7. It has been classified as problematic. Affected is the function filterKeyword. The manipulation of the argument value leads to resource consumption. VDB-231090 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3163**	N/A	A-RUO-RUOY-280623/590
Vendor: sailpoint					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: identityiq					
Affected Version(s): 8.1					
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	05-Jun-2023	8.8	IdentityIQ 8.3 and all 8.3 patch levels prior to 8.3p3, IdentityIQ 8.2 and all 8.2 patch levels prior to 8.2p6, IdentityIQ 8.1 and all 8.1 patch levels prior to 8.1p7, IdentityIQ 8.0 and all 8.0 patch levels prior to 8.0p6 allow an authenticated user to invoke a Java constructor with no arguments or a Java constructor with a single Map argument in any Java class available in the IdentityIQ application classpath. **CVE ID : CVE-2023-32217**	https://www.sailpoint.com/security-advisories/sailpoint-identityiq-unsafe-use-of-reflection-vulnerability-cve-2023-32217/	A-SAI-IDEN-280623/591
Affected Version(s): 8.2					
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	05-Jun-2023	8.8	IdentityIQ 8.3 and all 8.3 patch levels prior to 8.3p3, IdentityIQ 8.2 and all 8.2 patch levels prior to 8.2p6, IdentityIQ 8.1 and all 8.1 patch levels prior to 8.1p7, IdentityIQ 8.0 and all 8.0 patch levels prior to 8.0p6 allow an authenticated user to invoke a Java constructor with no	https://www.sailpoint.com/security-advisories/sailpoint-identityiq-unsafe-use-of-reflection-vulnerability-cve-2023-32217/	A-SAI-IDEN-280623/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arguments or a Java constructor with a single Map argument in any Java class available in the IdentityIQ application classpath. **CVE ID : CVE-2023-32217**		
Affected Version(s): 8.0					
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	05-Jun-2023	8.8	IdentityIQ 8.3 and all 8.3 patch levels prior to 8.3p3, IdentityIQ 8.2 and all 8.2 patch levels prior to 8.2p6, IdentityIQ 8.1 and all 8.1 patch levels prior to 8.1p7, IdentityIQ 8.0 and all 8.0 patch levels prior to 8.0p6 allow an authenticated user to invoke a Java constructor with no arguments or a Java constructor with a single Map argument in any Java class available in the IdentityIQ application classpath. **CVE ID : CVE-2023-32217**	https://www.sailpoint.com/security-advisories/sailpoint-identityiq-unsafe-use-of-reflection-vulnerability-cve-2023-32217/	A-SAI-IDEN-280623/593
Affected Version(s): 8.3					
Use of Externally-Controlled	05-Jun-2023	8.8	IdentityIQ 8.3 and all 8.3 patch levels prior to 8.3p3, IdentityIQ	https://www.sailpoint.com/security-	A-SAI-IDEN-280623/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input to Select Classes or Code ('Unsafe Reflection')			8.2 and all 8.2 patch levels prior to 8.2p6, IdentityIQ 8.1 and all 8.1 patch levels prior to 8.1p7, IdentityIQ 8.0 and all 8.0 patch levels prior to 8.0p6 allow an authenticated user to invoke a Java constructor with no arguments or a Java constructor with a single Map argument in any Java class available in the IdentityIQ application classpath. **CVE ID : CVE-2023-32217**	advisories/sailpoint-identityiq-unsafe-use-of-reflection-vulnerability-cve-2023-32217/	
Vendor: saison					
Product: dataspider_servista					
Affected Version(s): * Up to (including) 4.2					
Use of Hard-coded Credentials	01-Jun-2023	8.8	DataSpider Servista version 4.4 and earlier uses a hard-coded cryptographic key. DataSpider Servista is data integration software. ScriptRunner and ScriptRunner for Amazon SQS are used to start the configured processes on DataSpider Servista. The cryptographic key is embedded in ScriptRunner and ScriptRunner for	N/A	A-SAI-DATA-280623/595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Amazon SQS, which is common to all users. If an attacker who can gain access to a target DataSpider Servista instance and obtain a Launch Settings file of ScriptRunner and/or ScriptRunner for Amazon SQS, the attacker may perform operations with the user privilege encrypted in the file. Note that DataSpider Servista and some of the OEM products are affected by this vulnerability. For the details of affected products and versions, refer to the information listed in [References]. **CVE ID : CVE-2023-28937**		
Affected Version(s): 4.3					
Use of Hard-coded Credentials	01-Jun-2023	8.8	DataSpider Servista version 4.4 and earlier uses a hard-coded cryptographic key. DataSpider Servista is data integration software. ScriptRunner and ScriptRunner for Amazon SQS are used to start the configured processes on DataSpider Servista. The cryptographic key is embedded in ScriptRunner and	N/A	A-SAI-DATA-280623/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ScriptRunner for Amazon SQS, which is common to all users. If an attacker who can gain access to a target DataSpider Servista instance and obtain a Launch Settings file of ScriptRunner and/or ScriptRunner for Amazon SQS, the attacker may perform operations with the user privilege encrypted in the file. Note that DataSpider Servista and some of the OEM products are affected by this vulnerability. For the details of affected products and versions, refer to the information listed in [References]. **CVE ID : CVE-2023-28937**		
Affected Version(s): 4.4					
Use of Hard-coded Credentials	01-Jun-2023	8.8	DataSpider Servista version 4.4 and earlier uses a hard-coded cryptographic key. DataSpider Servista is data integration software. ScriptRunner and ScriptRunner for Amazon SQS are used to start the configured processes on DataSpider Servista. The cryptographic key is embedded in	N/A	A-SAI-DATA-280623/597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ScriptRunner and ScriptRunner for Amazon SQS, which is common to all users. If an attacker who can gain access to a target DataSpider Servista instance and obtain a Launch Settings file of ScriptRunner and/or ScriptRunner for Amazon SQS, the attacker may perform operations with the user privilege encrypted in the file. Note that DataSpider Servista and some of the OEM products are affected by this vulnerability. For the details of affected products and versions, refer to the information listed in [References]. **CVE ID : CVE-2023-28937**		
Vendor: salephpscripts					
Product: web_directory_free					
Affected Version(s): * Up to (including) 1.6.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	8.8	The Web Directory Free for WordPress is vulnerable to SQL Injection via the 'post_id' parameter in versions up to, and including, 1.6.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation	N/A	A-SAL-WEB_-280623/598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the existing SQL query. This makes it possible for authenticated attackers with contributor-level privileges to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-2201**		
Vendor: sales_tracker_management_system_project					
Product: sales_tracker_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	4.8	A vulnerability was found in SourceCodester Sales Tracker Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /classes/Users.php?f=save. The manipulation of the argument firstname/middlename/lastname/username leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-231164.	N/A	A-SAL-SALE-280623/599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3184		
Vendor: sendinblue					
Product: newsletter\,_smtp\,_email_marketing_and_subscribe					
Affected Version(s): * Up to (excluding) 3.1.61					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2023	6.1	The Newsletter, SMTP, Email marketing and Subscribe forms by Sendinblue WordPress plugin before 3.1.61 does not sanitise and escape a parameter before outputting it back in the admin dashboard when the WPML plugin is also active and configured, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-2472**	N/A	A-SEN-NEWS-280623/600
Vendor: service_provider_management_system_project					
Product: service_provider_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Jun-2023	9.8	Sourcecodester Service Provider Management System v1.0 is vulnerable to SQL Injection via the ID parameter in /php-spms/?page=services/view&id=2 **CVE ID : CVE-2023-34581**	N/A	A-SER-SERV-280623/601
Improper Neutralizat	06-Jun-2023	8.8	A vulnerability, which was classified as	N/A	A-SER-SERV-280623/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			critical, has been found in SourceCodester Service Provider Management System 1.0. Affected by this issue is some unknown functionality of the file view.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-230798 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3119**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jun-2023	7.2	A vulnerability, which was classified as critical, was found in SourceCodester Service Provider Management System 1.0. This affects an unknown part of the file view_service.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-230799.	N/A	A-SER-SERV-280623/603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3120		
Vendor: Siemens					
Product: jt2go					
Affected Version(s): * Up to (excluding) 14.2.0.2					
Stack-based Buffer Overflow	07-Jun-2023	7.8	Datalogics Library APDFLThe v18.0.4PlusP1e and prior contains a stack-based buffer overflow due to documents containing corrupted fonts, which could allow an attack that causes an unhandled crash during the rendering process. **CVE ID : CVE-2023-1709**	https://cert-portal.siemens.com/productcert/html/ssa-629917.html	A-SIE-JT2G-280623/604
Product: teamcenter_visualization					
Affected Version(s): From (including) 13.2.0 Up to (excluding) 13.2.0.13					
Stack-based Buffer Overflow	07-Jun-2023	7.8	Datalogics Library APDFLThe v18.0.4PlusP1e and prior contains a stack-based buffer overflow due to documents containing corrupted fonts, which could allow an attack that causes an unhandled crash during the rendering process.	https://cert-portal.siemens.com/productcert/html/ssa-629917.html	A-SIE-TEAM-280623/605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1709		
Affected Version(s): From (including) 13.3.0 Up to (excluding) 13.3.0.9					
Stack-based Buffer Overflow	07-Jun-2023	7.8	Datalogics Library APDFLThe v18.0.4PlusP1e and prior contains a stack-based buffer overflow due to documents containing corrupted fonts, which could allow an attack that causes an unhandled crash during the rendering process. **CVE ID : CVE-2023-1709**	https://cert-portal.siemens.com/productcert/html/ssa-629917.html	A-SIE-TEAM-280623/606
Affected Version(s): From (including) 14.0 Up to (excluding) 14.0.0.5					
Stack-based Buffer Overflow	07-Jun-2023	7.8	Datalogics Library APDFLThe v18.0.4PlusP1e and prior contains a stack-based buffer overflow due to documents containing corrupted fonts, which could allow an attack that causes an unhandled	https://cert-portal.siemens.com/productcert/html/ssa-629917.html	A-SIE-TEAM-280623/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash during the rendering process. **CVE ID : CVE-2023-1709**		
Affected Version(s): From (including) 14.1 Up to (excluding) 14.1.0.7					
Stack-based Buffer Overflow	07-Jun-2023	7.8	Datalogics Library APDFLThe v18.0.4PlusP1e and prior contains a stack-based buffer overflow due to documents containing corrupted fonts, which could allow an attack that causes an unhandled crash during the rendering process. **CVE ID : CVE-2023-1709**	https://cert-portal.siemens.com/productcert/html/ssa-629917.html	A-SIE-TEAM-280623/608
Affected Version(s): From (including) 14.2 Up to (excluding) 14.2.0.2					
Stack-based Buffer Overflow	07-Jun-2023	7.8	Datalogics Library APDFLThe v18.0.4PlusP1e and prior contains a stack-based buffer overflow due to documents containing corrupted fonts, which could allow an attack that	https://cert-portal.siemens.com/productcert/html/ssa-629917.html	A-SIE-TEAM-280623/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causes an unhandled crash during the rendering process. **CVE ID : CVE-2023-1709**		
Vendor: silabs					
Product: gecko_software_development_kit					
Affected Version(s): * Up to (including) 4.2.1					
Incorrect Calculation of Buffer Size	02-Jun-2023	3.3	Buffer overflow in Platform CLI component in Silicon Labs Gecko SDK v4.2.1 and earlier allows user to overwrite limited structures on the heap. **CVE ID : CVE-2023-2687**	N/A	A-SIL-GECK-280623/610
Vendor: simpleredak					
Product: simpleredak					
Affected Version(s): * Up to (excluding) 2.47.23.06					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jun-2023	9.8	eMedia Consulting simpleRedak up to v2.47.23.05 was discovered to contain a SQL injection vulnerability via the Activity parameter. **CVE ID : CVE-2023-33762**	N/A	A-SIM-SIMP-280623/611
Improper Neutralization of	02-Jun-2023	6.1	eMedia Consulting simpleRedak up to v2.47.23.05 was	N/A	A-SIM-SIMP-280623/612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /view/cb/format_642.php. **CVE ID : CVE-2023-33761**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-2023	6.1	eMedia Consulting simpleRedak up to v2.47.23.05 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /scheduler/index.php. **CVE ID : CVE-2023-33763**	N/A	A-SIM-SIMP-280623/613
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-2023	5.4	eMedia Consulting simpleRedak up to v2.47.23.05 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the component #/de/casting/show/detail/<ID>. **CVE ID : CVE-2023-33764**	N/A	A-SIM-SIMP-280623/614
Vendor: Sitecore					
Product: experience_platform					
Affected Version(s): 9.3					
Use of Externally-Controlled Input to Select Classes or	06-Jun-2023	8.8	Sitecore Experience Platform (XP) v9.3 was discovered to contain an authenticated remote code execution (RCE)	N/A	A-SIT-EXPE-280623/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Code ('Unsafe Reflection')			vulnerability via the component /sitecore/shell/Invoke.aspx. **CVE ID : CVE-2023-33652**		
N/A	06-Jun-2023	8.8	Sitecore Experience Platform (XP) v9.3 was discovered to contain an authenticated remote code execution (RCE) vulnerability via the component /Applications/Content%20Manager/Execute.aspx?cmd=convert&mode=HTML. **CVE ID : CVE-2023-33653**	N/A	A-SIT-EXPE-280623/616
Vendor: sogou					
Product: c\+\+_workflow					
Affected Version(s): 0.10.6					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jun-2023	8.8	In Sogou Workflow v0.10.6, memcpy a negtive size in URIParser::parse , may cause buffer-overflow and crash. **CVE ID : CVE-2023-33457**	https://github.com/sogou/workflow/issues/1272	A-SOG-C\+\-280623/617
Vendor: sonicjs					
Product: sonicjs					
Affected Version(s): From (including) 0.5.4 Up to (including) 0.7.0					
Improper Limitation of a Pathname to a	05-Jun-2023	6.5	SonicJS up to v0.7.0 allows attackers to execute an authenticated path traversal when an	https://github.com/lane711/sonicjs/pull/183	A-SON-SONI-280623/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			attacker injects special characters into the filename of a backup CMS. **CVE ID : CVE-2023-33690**		
Vendor: Southrivertech					
Product: titan_ftp_server_nextgen					
Affected Version(s): * Up to (excluding) 2.0.1.2102					
N/A	02-Jun-2023	8.8	An issue in South River Technologies TitanFTP Before v2.0.1.2102 allows attackers with low-level privileges to perform Administrative actions by sending requests to the user server. **CVE ID : CVE-2023-27745**	N/A	A-SOU-TITA-280623/619
Affected Version(s): * Up to (excluding) 2.1.0.2174					
N/A	02-Jun-2023	7.8	An issue was discovered in South River Technologies TitanFTP NextGen server that allows for a vertical privilege escalation leading to remote code execution. **CVE ID : CVE-2023-27744**	N/A	A-SOU-TITA-280623/620
Vendor: Splunk					
Product: splunk					
Affected Version(s): From (including) 8.1.0 Up to (excluding) 8.1.14					
N/A	01-Jun-2023	8.8	In versions of Splunk Enterprise below 9.0.5, 8.2.11, and	https://research.splunk.com/application/	A-SPL-SPLU-280623/621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.1.14, and Splunk Cloud Platform below version 9.0.2303.100, a low-privileged user who holds a role that has the 'edit_user' capability assigned to it can escalate their privileges to that of the admin user by providing specially crafted web requests. **CVE ID : CVE-2023-32707**	39e1c326-67d7-4c0d-8584-8056354f6593/, https://advisory.splunk.com/advisories/SVD-2023-0602	
Interpretation Conflict	01-Jun-2023	8.8	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, and Splunk Cloud Platform versions below 9.0.2303.100, a low-privileged user can trigger an HTTP response splitting vulnerability with the 'rest' SPL command that lets them potentially access other REST endpoints in the system arbitrarily. **CVE ID : CVE-2023-32708**	https://research.splunk.com/application/e615a0e1-a1b2-4196-9865-8aa646e1708c/, https://advisory.splunk.com/advisories/SVD-2023-0603	A-SPL-SPLU-280623/622
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Jun-2023	8.1	In the Splunk App for Lookup File Editing versions below 4.0.1, a low-privileged user can, with a specially crafted web request, trigger a path traversal exploit that can then be used to read and write to restricted areas of the	https://advisory.splunk.com/advisories/SVD-2023-0608, https://research.splunk.com/application/8ed58987-738d-4917-9e44-	A-SPL-SPLU-280623/623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Splunk installation directory. **CVE ID : CVE-2023-32714**	b8ef6ab948a6/	
Improper Restriction of XML External Entity Reference	01-Jun-2023	6.5	On Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, an unauthenticated attacker can send specially-crafted messages to the XML parser within SAML authentication to cause a denial of service in the Splunk daemon. **CVE ID : CVE-2023-32706**	https://advisory.splunk.com/advisories/SVD-2023-0601	A-SPL-SPLU-280623/624
Improper Check for Unusual or Exceptional Conditions	01-Jun-2023	6.5	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, and Splunk Cloud Platform versions below 9.0.2303.100, an attacker can exploit a vulnerability in the {{dump}} SPL command to cause a denial of service by crashing the Splunk daemon. **CVE ID : CVE-2023-32716**	https://advisory.splunk.com/advisories/SVD-2023-0611, https://research.splunk.com/application/fb0e6823-365f-48ed-b09e-272ac4c1dad6/	A-SPL-SPLU-280623/625
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-2023	5.4	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, a Splunk dashboard view lets a low-privileged user exploit a vulnerability in the Bootstrap web framework (CVE-	https://research.splunk.com/application/8a43558f-a53c-4ee4-86c1-30b1e8ef3606/, https://advis	A-SPL-SPLU-280623/626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2019-8331) and build a stored cross-site scripting (XSS) payload. **CVE ID : CVE-2023-32711**	ory.splunk.com/advisories/SVD-2023-0605	
N/A	01-Jun-2023	5.3	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, and in Splunk Cloud Platform versions below 9.0.2303.100, a low-privileged user can perform an unauthorized transfer of data from a search using the 'copyresults' command if they know the search ID (SID) of a search job that has recently run. **CVE ID : CVE-2023-32710**	https://advisory.splunk.com/advisories/SVD-2023-0609	A-SPL-SPLU-280623/627
N/A	01-Jun-2023	4.3	In Splunk Enterprise versions below 9.0.5, 8.2.11. and 8.1.14, and Splunk Cloud Platform versions below 9.0.2303.100, a low-privileged user who holds the 'user' role can see the hashed version of the initial user name and password for the Splunk instance by using the 'rest' SPL command against the 'conf-user-seed' REST endpoint. **CVE ID : CVE-2023-32709**	https://research.splunk.com/application/a1be424d-e59c-4583-b6f9-2dcc23be4875/, https://advisory.splunk.com/advisories/SVD-2023-0604	A-SPL-SPLU-280623/628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Jun-2023	4.3	On Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, and in Splunk Cloud Platform versions below 9.0.2303.100, an unauthorized user can access the {{/services/indexing/preview}} REST endpoint to overwrite search results if they know the search ID (SID) of an existing search job. **CVE ID : CVE-2023-32717**	https://research.splunk.com/application/bbe26f95-1655-471d-8abd-3d32fafa86f8/, https://advisory.splunk.com/advisories/SVD-2023-0612	A-SPL-SPLU-280623/629
Improper Encoding or Escaping of Output	01-Jun-2023	3.1	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, an attacker can use a specially crafted web URL in their browser to cause log file poisoning. The attack requires the attacker to have secure shell (SSH) access to the instance and use a terminal program that supports a certain feature set to execute the attack successfully. **CVE ID : CVE-2023-32712**	https://advisory.splunk.com/advisories/SVD-2023-0606	A-SPL-SPLU-280623/630
Affected Version(s): From (including) 8.2.0 Up to (excluding) 8.2.11					
N/A	01-Jun-2023	8.8	In versions of Splunk Enterprise below 9.0.5, 8.2.11, and 8.1.14, and Splunk Cloud Platform below	https://research.splunk.com/application/39e1c326-67d7-4c0d-	A-SPL-SPLU-280623/631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 9.0.2303.100, a low-privileged user who holds a role that has the 'edit_user' capability assigned to it can escalate their privileges to that of the admin user by providing specially crafted web requests. **CVE ID : CVE-2023-32707**	8584-8056354f6593/, https://advisory.splunk.com/advisories/SVD-2023-0602	
Interpretation Conflict	01-Jun-2023	8.8	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, and Splunk Cloud Platform versions below 9.0.2303.100, a low-privileged user can trigger an HTTP response splitting vulnerability with the 'rest' SPL command that lets them potentially access other REST endpoints in the system arbitrarily. **CVE ID : CVE-2023-32708**	https://research.splunk.com/application/e615a0e1-a1b2-4196-9865-8aa646e1708c/, https://advisory.splunk.com/advisories/SVD-2023-0603	A-SPL-SPLU-280623/632
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Jun-2023	8.1	In the Splunk App for Lookup File Editing versions below 4.0.1, a low-privileged user can, with a specially crafted web request, trigger a path traversal exploit that can then be used to read and write to restricted areas of the	https://advisory.splunk.com/advisories/SVD-2023-0608, https://research.splunk.com/application/8ed58987-738d-4917-9e44-	A-SPL-SPLU-280623/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Splunk installation directory. **CVE ID : CVE-2023-32714**	b8ef6ab948a6/	
Improper Restriction of XML External Entity Reference	01-Jun-2023	6.5	On Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, an unauthenticated attacker can send specially-crafted messages to the XML parser within SAML authentication to cause a denial of service in the Splunk daemon. **CVE ID : CVE-2023-32706**	https://advisory.splunk.com/advisories/SVD-2023-0601	A-SPL-SPLU-280623/634
Improper Check for Unusual or Exceptional Conditions	01-Jun-2023	6.5	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, and Splunk Cloud Platform versions below 9.0.2303.100, an attacker can exploit a vulnerability in the {{dump}} SPL command to cause a denial of service by crashing the Splunk daemon. **CVE ID : CVE-2023-32716**	https://advisory.splunk.com/advisories/SVD-2023-0611, https://research.splunk.com/application/fb0e6823-365f-48ed-b09e-272ac4c1dad6/	A-SPL-SPLU-280623/635
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-2023	5.4	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, a Splunk dashboard view lets a low-privileged user exploit a vulnerability in the Bootstrap web framework (CVE-	https://research.splunk.com/application/8a43558f-a53c-4ee4-86c1-30b1e8ef3606/, https://advis	A-SPL-SPLU-280623/636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2019-8331) and build a stored cross-site scripting (XSS) payload. **CVE ID : CVE-2023-32711**	ory.splunk.com/advisories/SVD-2023-0605	
N/A	01-Jun-2023	5.3	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, and in Splunk Cloud Platform versions below 9.0.2303.100, a low-privileged user can perform an unauthorized transfer of data from a search using the 'copyresults' command if they know the search ID (SID) of a search job that has recently run. **CVE ID : CVE-2023-32710**	https://advisory.splunk.com/advisories/SVD-2023-0609	A-SPL-SPLU-280623/637
N/A	01-Jun-2023	4.3	In Splunk Enterprise versions below 9.0.5, 8.2.11. and 8.1.14, and Splunk Cloud Platform versions below 9.0.2303.100, a low-privileged user who holds the 'user' role can see the hashed version of the initial user name and password for the Splunk instance by using the 'rest' SPL command against the 'conf-user-seed' REST endpoint. **CVE ID : CVE-2023-32709**	https://research.splunk.com/application/a1be424d-e59c-4583-b6f9-2dcc23be4875/, https://advisory.splunk.com/advisories/SVD-2023-0604	A-SPL-SPLU-280623/638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Jun-2023	4.3	On Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, and in Splunk Cloud Platform versions below 9.0.2303.100, an unauthorized user can access the {{/services/indexing/preview}} REST endpoint to overwrite search results if they know the search ID (SID) of an existing search job. **CVE ID : CVE-2023-32717**	https://research.splunk.com/application/bbe26f95-1655-471d-8abd-3d32fafa86f8/, https://advisory.splunk.com/advisories/SVD-2023-0612	A-SPL-SPLU-280623/639
Improper Encoding or Escaping of Output	01-Jun-2023	3.1	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, an attacker can use a specially crafted web URL in their browser to cause log file poisoning. The attack requires the attacker to have secure shell (SSH) access to the instance and use a terminal program that supports a certain feature set to execute the attack successfully. **CVE ID : CVE-2023-32712**	https://advisory.splunk.com/advisories/SVD-2023-0606	A-SPL-SPLU-280623/640
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.0.5					
N/A	01-Jun-2023	8.8	In versions of Splunk Enterprise below 9.0.5, 8.2.11, and 8.1.14, and Splunk Cloud Platform below	https://research.splunk.com/application/39e1c326-67d7-4c0d-	A-SPL-SPLU-280623/641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 9.0.2303.100, a low-privileged user who holds a role that has the 'edit_user' capability assigned to it can escalate their privileges to that of the admin user by providing specially crafted web requests. **CVE ID : CVE-2023-32707**	8584-8056354f6593/, https://advisory.splunk.com/advisories/SVD-2023-0602	
Interpretation Conflict	01-Jun-2023	8.8	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, and Splunk Cloud Platform versions below 9.0.2303.100, a low-privileged user can trigger an HTTP response splitting vulnerability with the 'rest' SPL command that lets them potentially access other REST endpoints in the system arbitrarily. **CVE ID : CVE-2023-32708**	https://research.splunk.com/application/e615a0e1-a1b2-4196-9865-8aa646e1708c/, https://advisory.splunk.com/advisories/SVD-2023-0603	A-SPL-SPLU-280623/642
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Jun-2023	8.1	In the Splunk App for Lookup File Editing versions below 4.0.1, a low-privileged user can, with a specially crafted web request, trigger a path traversal exploit that can then be used to read and write to restricted areas of the	https://advisory.splunk.com/advisories/SVD-2023-0608, https://research.splunk.com/application/8ed58987-738d-4917-9e44-	A-SPL-SPLU-280623/643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Splunk installation directory. **CVE ID : CVE-2023-32714**	b8ef6ab948a6/	
Improper Restriction of XML External Entity Reference	01-Jun-2023	6.5	On Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, an unauthenticated attacker can send specially-crafted messages to the XML parser within SAML authentication to cause a denial of service in the Splunk daemon. **CVE ID : CVE-2023-32706**	https://advisory.splunk.com/advisories/SVD-2023-0601	A-SPL-SPLU-280623/644
Improper Check for Unusual or Exceptional Conditions	01-Jun-2023	6.5	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, and Splunk Cloud Platform versions below 9.0.2303.100, an attacker can exploit a vulnerability in the {{dump}} SPL command to cause a denial of service by crashing the Splunk daemon. **CVE ID : CVE-2023-32716**	https://advisory.splunk.com/advisories/SVD-2023-0611, https://research.splunk.com/application/fb0e6823-365f-48ed-b09e-272ac4c1dad6/	A-SPL-SPLU-280623/645
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-2023	5.4	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, a Splunk dashboard view lets a low-privileged user exploit a vulnerability in the Bootstrap web framework (CVE-	https://research.splunk.com/application/8a43558f-a53c-4ee4-86c1-30b1e8ef3606/, https://advis	A-SPL-SPLU-280623/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2019-8331) and build a stored cross-site scripting (XSS) payload. **CVE ID : CVE-2023-32711**	ory.splunk.com/advisories/SVD-2023-0605	
N/A	01-Jun-2023	5.3	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, and in Splunk Cloud Platform versions below 9.0.2303.100, a low-privileged user can perform an unauthorized transfer of data from a search using the 'copyresults' command if they know the search ID (SID) of a search job that has recently run. **CVE ID : CVE-2023-32710**	https://advisory.splunk.com/advisories/SVD-2023-0609	A-SPL-SPLU-280623/647
N/A	01-Jun-2023	4.3	In Splunk Enterprise versions below 9.0.5, 8.2.11. and 8.1.14, and Splunk Cloud Platform versions below 9.0.2303.100, a low-privileged user who holds the 'user' role can see the hashed version of the initial user name and password for the Splunk instance by using the 'rest' SPL command against the 'conf-user-seed' REST endpoint. **CVE ID : CVE-2023-32709**	https://research.splunk.com/application/a1be424d-e59c-4583-b6f9-2dcc23be4875/, https://advisory.splunk.com/advisories/SVD-2023-0604	A-SPL-SPLU-280623/648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Jun-2023	4.3	On Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, and in Splunk Cloud Platform versions below 9.0.2303.100, an unauthorized user can access the {{/services/indexing/preview}} REST endpoint to overwrite search results if they know the search ID (SID) of an existing search job. **CVE ID : CVE-2023-32717**	https://research.splunk.com/application/bbe26f95-1655-471d-8abd-3d32fafa86f8/, https://advisory.splunk.com/advisories/SVD-2023-0612	A-SPL-SPLU-280623/649
Improper Encoding or Escaping of Output	01-Jun-2023	3.1	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, an attacker can use a specially crafted web URL in their browser to cause log file poisoning. The attack requires the attacker to have secure shell (SSH) access to the instance and use a terminal program that supports a certain feature set to execute the attack successfully. **CVE ID : CVE-2023-32712**	https://advisory.splunk.com/advisories/SVD-2023-0606	A-SPL-SPLU-280623/650
Product: splunk_app_for_lookup_file_editing					
Affected Version(s): * Up to (excluding) 4.0.1					
Improper Limitation of a Pathname	01-Jun-2023	8.1	In the Splunk App for Lookup File Editing versions below 4.0.1, a low-privileged user	https://advisory.splunk.com/advisories/SVD-2023-	A-SPL-SPLU-280623/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			can, with a specially crafted web request, trigger a path traversal exploit that can then be used to read and write to restricted areas of the Splunk installation directory. **CVE ID : CVE-2023-32714**	0608, https://research.splunk.com/application/8ed58987-738d-4917-9e44-b8ef6ab948a6/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jun-2023	6.1	In the Splunk App for Lookup File Editing versions below 4.0.1, a user can insert potentially malicious JavaScript code into the app, which causes that code to run on the user's machine. The app itself does not contain the potentially malicious JavaScript code. The vulnerability requires the attacker to phish the victim by tricking them into initiating a request within their browser, and requires additional user interaction to trigger. The attacker cannot exploit the vulnerability at will. **CVE ID : CVE-2023-32715**	https://advisory.splunk.com/advisories/SVD-2023-0610	A-SPL-SPLU-280623/652
Product: splunk_app_for_stream					
Affected Version(s): * Up to (excluding) 8.1.1					
Improper Privilege	01-Jun-2023	9.9	In Splunk App for Stream versions below 8.1.1, a low-	https://advisory.splunk.com/advisories	A-SPL-SPLU-280623/653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			privileged user could use a vulnerability in the streamfwd process within the Splunk App for Stream to escalate their privileges on the machine that runs the Splunk Enterprise instance, up to and including the root user. **CVE ID : CVE-2023-32713**	/SVD-2023-0607	
Product: splunk_cloud_platform					
Affected Version(s): * Up to (excluding) 9.0.2303.100					
N/A	01-Jun-2023	8.8	In versions of Splunk Enterprise below 9.0.5, 8.2.11, and 8.1.14, and Splunk Cloud Platform below version 9.0.2303.100, a low-privileged user who holds a role that has the 'edit_user' capability assigned to it can escalate their privileges to that of the admin user by providing specially crafted web requests. **CVE ID : CVE-2023-32707**	https://research.splunk.com/application/39e1c326-67d7-4c0d-8584-8056354f6593/, https://advisory.splunk.com/advisories/SVD-2023-0602	A-SPL-SPLU-280623/654
Interpretation Conflict	01-Jun-2023	8.8	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, and Splunk Cloud Platform versions below 9.0.2303.100, a low-privileged user can trigger an HTTP response splitting vulnerability with the	https://research.splunk.com/application/e615a0e1-a1b2-4196-9865-8aa646e1708c/, https://advisory.splunk.co	A-SPL-SPLU-280623/655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'rest' SPL command that lets them potentially access other REST endpoints in the system arbitrarily. **CVE ID : CVE-2023-32708**	m/advisories/SVD-2023-0603	
Improper Restriction of XML External Entity Reference	01-Jun-2023	6.5	On Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, an unauthenticated attacker can send specially-crafted messages to the XML parser within SAML authentication to cause a denial of service in the Splunk daemon. **CVE ID : CVE-2023-32706**	https://advisory.splunk.com/advisories/SVD-2023-0601	A-SPL-SPLU-280623/656
Improper Check for Unusual or Exceptional Conditions	01-Jun-2023	6.5	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, and Splunk Cloud Platform versions below 9.0.2303.100, an attacker can exploit a vulnerability in the {{dump}} SPL command to cause a denial of service by crashing the Splunk daemon. **CVE ID : CVE-2023-32716**	https://advisory.splunk.com/advisories/SVD-2023-0611, https://research.splunk.com/application/fb0e6823-365f-48ed-b09e-272ac4c1dad6/	A-SPL-SPLU-280623/657
N/A	01-Jun-2023	5.3	In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, and in Splunk Cloud Platform versions	https://advisory.splunk.com/advisories/SVD-2023-0609	A-SPL-SPLU-280623/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below 9.0.2303.100, a low-privileged user can perform an unauthorized transfer of data from a search using the 'copyresults' command if they know the search ID (SID) of a search job that has recently run. **CVE ID : CVE-2023-32710**		
N/A	01-Jun-2023	4.3	In Splunk Enterprise versions below 9.0.5, 8.2.11. and 8.1.14, and Splunk Cloud Platform versions below 9.0.2303.100, a low-privileged user who holds the 'user' role can see the hashed version of the initial user name and password for the Splunk instance by using the 'rest' SPL command against the 'conf-user-seed' REST endpoint. **CVE ID : CVE-2023-32709**	https://research.splunk.com/application/a1be424d-e59c-4583-b6f9-2dcc23be4875/, https://advisory.splunk.com/advisories/SVD-2023-0604	A-SPL-SPLU-280623/659
N/A	01-Jun-2023	4.3	On Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, and in Splunk Cloud Platform versions below 9.0.2303.100, an unauthorized user can access the {{/services/indexing/preview}} REST endpoint to overwrite search results if they	https://research.splunk.com/application/bbe26f95-1655-471d-8abd-3d32fafa86f8/, https://advisory.splunk.com/advisories	A-SPL-SPLU-280623/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			know the search ID (SID) of an existing search job. **CVE ID : CVE-2023-32717**	/SVD-2023-0612	
Vendor: Status					
Product: powerbpm					
Affected Version(s): 2.0					
Missing Authentication for Critical Function	02-Jun-2023	5.7	It is identified a vulnerability of insufficient authentication in an important specific function of Status PowerBPM. A LAN attacker with normal user privilege can exploit this vulnerability to modify substitute agent to arbitrary users, resulting in serious consequence. **CVE ID : CVE-2023-25780**	N/A	A-STA-POWE-280623/661
Vendor: staxwp					
Product: stax					
Affected Version(s): * Up to (including) 1.4.3					
Missing Authorization	09-Jun-2023	4.3	The Elementor Addons, Widgets and Enhancements – Stax plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the toggle_widget function in versions up to, and including, 1.4.3. This makes it	N/A	A-STA-STAX-280623/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible for authenticated attackers, with subscriber-level permissions and above, to enable or disable Elementor widgets. **CVE ID : CVE-2023-2189**		
Vendor: story_saver_for_instagram_-_video_downloader_project					
Product: story_saver_for_instagram_-_video_downloader					
Affected Version(s): 1.0.6					
N/A	01-Jun-2023	7.5	Story Saver for Instragram - Video Downloader 1.0.6 for Android has an exposed component that provides a method to modify the SharedPreference file. An attacker can leverage this method to inject a large amount of data into any SharedPreference file, which will be loaded into memory when the application is opened. When an attacker injects too much data, the application will trigger an OOM error and crash at startup, resulting in a persistent denial of service. **CVE ID : CVE-2023-29748**	N/A	A-STO-STOR-280623/663
Vendor: stpetedesign					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: call_now_accessibility_button					
Affected Version(s): * Up to (including) 1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jun-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in StPeteDesign Call Now Accessibility Button plugin <= 1.1 versions. **CVE ID : CVE-2023-28933**	N/A	A-STP-CALL-280623/664
Vendor: supsystic					
Product: easy_google_maps					
Affected Version(s): * Up to (including) 1.11.7					
Cross-Site Request Forgery (CSRF)	09-Jun-2023	5.4	The Easy Google Maps plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.11.7. This is due to missing or incorrect nonce validation on the AJAX action handler. This makes it possible for unauthenticated attackers to executes AJAX actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-2526**	https://plugins.trac.wordpress.org/changeset/2916430/, https://plugins.trac.wordpress.org/changeset/2916430/google-maps-easy/trunk/classes/frame.php?contextall=1	A-SUP-EASY-280623/665
Vendor: Suse					
Product: rancher					
Affected Version(s): From (including) 2.6.0 Up to (excluding) 2.6.13					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Preservation of Permissions	01-Jun-2023	8	An Improper Privilege Management vulnerability in SUSE Rancher allowed standard users to leverage their existing permissions to manipulate Kubernetes secrets in the local cluster, resulting in the secret being deleted, but their read-level permissions to the secret being preserved. When this operation was followed-up by other specially crafted commands, it could result in the user gaining access to tokens belonging to service accounts in the local cluster. This issue affects Rancher: from >= 2.6.0 before < 2.6.13, from >= 2.7.0 before < 2.7.4. **CVE ID : CVE-2023-22647**	https://github.com/rancher/rancher/security/advisories/GHSA-p976-h52c-26p6, https://bugzilla.suse.com/show_bug.cgi?id=CVE-2023-22647	A-SUS-RANC-280623/666
Affected Version(s): From (including) 2.6.7 Up to (excluding) 2.6.13					
Session Fixation	01-Jun-2023	8.8	A Improper Privilege Management	https://github.com/ranche	A-SUS-RANC-280623/667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in SUSE Rancher causes permission changes in Azure AD not to be reflected to users while they are logged in the Rancher UI. This would cause the users to retain their previous permissions in Rancher, even if they change groups on Azure AD, for example, to a lower privileged group, or are removed from a group, thus retaining their access to Rancher instead of losing it. This issue affects Rancher: from >= 2.6.7 before < 2.6.13, from >= 2.7.0 before < 2.7.4. **CVE ID : CVE-2023-22648**	r/rancher/security/advisories/GHSA-vf6j-6739-78m8, https://bugzilla.suse.com/show_bug.cgi?id=CVE-2023-22648	
Affected Version(s): From (including) 2.7.0 Up to (excluding) 2.7.4					
Session Fixation	01-Jun-2023	8.8	A Improper Privilege Management vulnerability in SUSE Rancher causes permission changes in Azure AD not to be reflected to users	https://github.com/rancher/rancher/security/advisories/GHSA-vf6j-6739-78m8, https://bugzilla.suse.com/s	A-SUS-RANC-280623/668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while they are logged in the Rancher UI. This would cause the users to retain their previous permissions in Rancher, even if they change groups on Azure AD, for example, to a lower privileged group, or are removed from a group, thus retaining their access to Rancher instead of losing it. This issue affects Rancher: from >= 2.6.7 before < 2.6.13, from >= 2.7.0 before < 2.7.4. **CVE ID : CVE-2023-22648**	how_bug.cgi?id=CVE-2023-22648	
Improper Preservation of Permissions	01-Jun-2023	8	An Improper Privilege Management vulnerability in SUSE Rancher allowed standard users to leverage their existing permissions to manipulate Kubernetes secrets in the local cluster, resulting in the secret being deleted, but their read-level	https://github.com/rancher/rancher/security/advisories/GHSA-p976-h52c-26p6, https://bugzilla.suse.com/show_bug.cgi?id=CVE-2023-22647	A-SUS-RANC-280623/669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permissions to the secret being preserved. When this operation was followed-up by other specially crafted commands, it could result in the user gaining access to tokens belonging to service accounts in the local cluster. This issue affects Rancher: from >= 2.6.0 before < 2.6.13, from >= 2.7.0 before < 2.7.4. **CVE ID : CVE-2023-22647**		
Vendor: tdengine					
Product: grafana					
Affected Version(s): * Up to (including) 2023-05-22					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jun-2023	9.8	The `Release PR Merged` workflow in the github repo taosdata/grafanaplugin is subject to a command injection vulnerability which allows for arbitrary code execution within the github action context due to the insecure usage of `${{ github.event.pull_request.title }}` in a bash	N/A	A-TDE-GRAF-280623/670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command within the GitHub workflow. Attackers can inject malicious commands which will be executed by the workflow. This happens because `${{ github.event.pull_request.title }}` is directly passed to bash command on like 25 of the workflow. This may allow an attacker to gain access to secrets which the github action has access to or to otherwise make use of the compute resources. **CVE ID : CVE-2023-34111**		
Vendor: teachers_record_management_system_project					
Product: teachers_record_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	09-Jun-2023	5.4	A vulnerability, which was classified as critical, has been found in PHPGurukul Teachers Record Management System 1.0. Affected by this issue is some unknown functionality of the file /changeimage.php of the component Profile Picture Handler. The manipulation of the argument newpic leads to unrestricted upload. The attack	N/A	A-TEA-TEAC-280623/671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-231176. **CVE ID : CVE-2023-3187**		
Vendor: Teampass					
Product: teampass					
Affected Version(s): * Up to (excluding) 3.0.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-2023	9	Cross-site Scripting (XSS) - Stored in GitHub repository nilsteampassnet/teampass prior to 3.0.9. **CVE ID : CVE-2023-3086**	https://huntr.dev/bounties/17be9e8a-abe8-41db-987f-1d5b0686ae20, https://github.com/nilsteampassnet/teampass/commit/1c0825b67eb8f8b5ecc418ff7614423a275e6a79	A-TEA-TEAM-280623/672
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-2023	8.7	Cross-site Scripting (XSS) - Stored in GitHub repository nilsteampassnet/teampass prior to 3.0.9. **CVE ID : CVE-2023-3083**	https://github.com/nilsteampassnet/teampass/commit/79731553fa305d45dabb7a227f3074d56d7c94c1, https://huntr.dev/bounties/c6b29e46-02e0-43ad-920f-28ac482ea2ab	A-TEA-TEAM-280623/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-2023	8.1	Cross-site Scripting (XSS) - Stored in GitHub repository nilsteampassnet/teampass prior to 3.0.9. **CVE ID : CVE-2023-3084**	https://github.com/nilsteampassnet/teampass/commit/61b9b7d4e33bbaad2cd61a7ee988f9c22298bf1a, https://huntr.dev/bounties/4b86b56b-c51b-4be8-8ee4-6e385d1e9e8a	A-TEA-TEAM-280623/674
Improper Access Control	04-Jun-2023	6.5	Improper Access Control in GitHub repository nilsteampassnet/teampass prior to 3.0.9. **CVE ID : CVE-2023-3095**	https://huntr.dev/bounties/35c899a9-40a0-4e17-bfb5-2a1430bc83c4, https://github.com/nilsteampassnet/teampass/commit/774985f62f080715774604927fba2cb6ef701612	A-TEA-TEAM-280623/675
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jun-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository nilsteampassnet/teampass prior to 3.0.9. **CVE ID : CVE-2023-3191**	https://github.com/nilsteampassnet/teampass/commit/241dbd4159a5d63b55af426464d30dbb53925705, https://huntr.dev/bounties/19fed157-128d-4bfb-	A-TEA-TEAM-280623/676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				a30e-eadf748cbd1a	
Improper Encoding or Escaping of Output	10-Jun-2023	4.6	Improper Encoding or Escaping of Output in GitHub repository nilsteampassnet/teampass prior to 3.0.9. **CVE ID : CVE-2023-3190**	https://huntr.dev/bounties/5562c4c4-0475-448f-a451-7c4666bc7180, https://github.com/nilsteampassnet/teampass/commit/241dbd4159a5d63b55af426464d30dbb53925705	A-TEA-TEAM-280623/677
Vendor: Tencent					
Product: qq					
Affected Version(s): From (including) 9.7.1.28940 Up to (including) 9.7.8.29039					
Release of Invalid Pointer or Reference	01-Jun-2023	7.8	In Tencent QQ through 9.7.8.29039 and TIM through 3.4.7.22084, QQProtect.exe and QQProtectEngine.dll do not validate pointers from inter-process communication, which leads to a write-what-where condition. **CVE ID : CVE-2023-34312**	N/A	A-TEN-QQ-280623/678
Product: tim					
Affected Version(s): From (including) 3.4.5.22071 Up to (including) 3.4.7.22084					
Release of Invalid Pointer or Reference	01-Jun-2023	7.8	In Tencent QQ through 9.7.8.29039 and TIM through 3.4.7.22084, QQProtect.exe and	N/A	A-TEN-TIM-280623/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QQProtectEngine.dll do not validate pointers from inter-process communication, which leads to a write-what-where condition. **CVE ID : CVE-2023-34312**		
Vendor: tgstation13					
Product: tgstation-server					
Affected Version(s): From (including) 4.0.0.0 Up to (excluding) 5.12.5					
Improper Restriction of Excessive Authentication Attempts	08-Jun-2023	5.3	TGstation is a toolset to manage production BYOND servers. In affected versions if a Windows user was registered in tgstation-server (TGS), an attacker could discover their username by brute-forcing the login endpoint with an invalid password. When a valid Windows logon was found, a distinct response would be generated. This issue has been addressed in version 5.12.5. Users are advised to upgrade. Users unable to upgrade may be mitigated by rate-limiting API calls with software that sits in front of TGS in the HTTP pipeline such as fail2ban.	https://github.com/tgstation/tgstation-server/pull/1526, https://github.com/tgstation/tgstation-server/security/advisories/GHSA-w3jx-4x93-76ph	A-TGS-TGST-280623/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34243		
Vendor: themefic					
Product: ultimate_addons_for_contact_form_7					
Affected Version(s): * Up to (including) 3.1.23					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Jun-2023	6.5	The Ultimate Addons for Contact Form 7 plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter in versions up to, and including, 3.1.23. This makes it possible for authenticated attackers of any authorization level to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-1615**	https://plugins.trac.wordpress.org/changeset/2901676/, https://plugins.trac.wordpress.org/browser/ultimate-addons-for-contact-form-7/trunk/addons/database/database.php?rev=2897709#L255	A-THE-ULTI-280623/681
Vendor: themeisle					
Product: multiple_page_generator					
Affected Version(s): * Up to (including) 3.3.17					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Jun-2023	7.2	The Multiple Page Generator Plugin for WordPress is vulnerable to time-based SQL Injection via the orderby and order parameters in versions up to, and including, 3.3.17 due to insufficient escaping on the user supplied parameter and lack of sufficient	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2910686%40multiple-pages-generator-by-porthas%2Ftrunk&old=2905353%40mul	A-THE-MULT-280623/682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			preparation on the existing SQL query. This makes it possible for authenticated attackers with administrator privileges to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-2607**	tiple-pages-generator-by-porthas%2Ftrunk&sfp_email=&sfph_mail=	
Vendor: thethaiger					
Product: the_thaiger					
Affected Version(s): 1.2					
N/A	02-Jun-2023	9.8	An issue found in The Thaiger v.1.2 for Android allows unauthorized apps to cause a code execution attack by manipulating the SharedPreference files. **CVE ID : CVE-2023-29746**	N/A	A-THE-THE_-280623/683
Vendor: this_day_in_history_project					
Product: this_day_in_history					
Affected Version(s): * Up to (including) 3.10.1					
Improper Neutralization of Input During Web Page Generation	12-Jun-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in BrokenCrust This Day In History plugin <= 3.10.1 versions. **CVE ID : CVE-2023-34026**	N/A	A-THI-THIS-280623/684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
Vendor: timmystudios					
Product: keyboard_themes					
Affected Version(s): 1.275.1.164					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Jun-2023	9.8	Keyboard Themes 1.275.1.164 for Android contains a dictionary traversal vulnerability that allows unauthorized apps to overwrite arbitrary files in its internal storage and achieve arbitrary code execution. **CVE ID : CVE-2023-29736**	N/A	A-TIM-KEYB-280623/685
Vendor: trellix					
Product: agent					
Affected Version(s): * Up to (excluding) 5.7.9					
Out-of-bounds Write	07-Jun-2023	8.1	A heap-based overflow vulnerability in TA prior to version 5.7.9 allows a remote user to alter the page heap in the macmnsvc process memory block, resulting in the service becoming unavailable. **CVE ID : CVE-2023-1388**	https://kcm.trellix.com/corporate/index?page=content&id=SB10398	A-TRE-AGEN-280623/686
Uncontrolled Search	07-Jun-2023	7.8	A command Injection Vulnerability in TA for	https://kcm.trellix.com/corporate/index?	A-TRE-AGEN-280623/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Path Element			mac-OS prior to version 5.7.9 allows local users to place an arbitrary file into the /Library/Trellix/Agent/bin/ folder. The malicious file is executed by running the TA deployment feature located in the System Tree. **CVE ID : CVE-2023-0976**	page=content&id=SB10398	
Vendor: trilium_project					
Product: trilium					
Affected Version(s): * Up to (excluding) 0.59.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository zadam/trilium prior to 0.59.4. **CVE ID : CVE-2023-3067**	https://github.com/zadam/trilium/commit/4c3fcc3ea6f37debcb87ac1a7f5698c27be0e67b, https://huntr.dev/bounties/4772ceb7-1594-414d-9b20-5b82029da7b6	A-TRI-TRIL-280623/688
Vendor: trumani					
Product: stop_spammers					
Affected Version(s): * Up to (excluding) 2023					
Improper Neutralization of Input During	05-Jun-2023	6.1	The Stop Spammers Security | Block Spam Users, Comments, Forms WordPress plugin before 2023	N/A	A-TRU-STOP-280623/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			does not sanitise and escape various parameters before outputting them back in admin dashboard pages, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-2488**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2023	4.8	The Stop Spammers Security | Block Spam Users, Comments, Forms WordPress plugin before 2023 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-2023-2489**	N/A	A-TRU-STOP-280623/690
Vendor: tshirtecommerce					
Product: custom_product_designer					
Affected Version(s): * Up to (including) 2.1.4					
Improper Limitation of a Pathname to a Restricted	01-Jun-2023	7.5	An issue was discovered in the tshirtecommerce (aka Custom Product Designer) component 2.1.4 for PrestaShop.	https://friends-of-presta.github.io/security-advisories/module/2023/0	A-TSH-CUST-280623/691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			An HTTP request can be forged with the POST parameter file_name in the tshirtecommerce/ajax.php?type=svg endpoint, to allow a remote attacker to traverse directories on the system in order to open files (without restriction on the extension and path). Only files that can be parsed in XML can be opened. This is exploited in the wild in March 2023. **CVE ID : CVE-2023-27639**	3/30/tshirtecommerce_cwe-22.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Jun-2023	7.5	An issue was discovered in the tshirtecommerce (aka Custom Product Designer) component 2.1.4 for PrestaShop. An HTTP request can be forged with the POST parameter type in the /tshirtecommerce/fonts.php endpoint, to allow a remote attacker to traverse directories on the system in order to open files (without restriction on the extension and path). The content of the file is returned with base64 encoding. This	https://friends-of-presta.github.io/security-advisories/module/2023/03/30/tshirtecommerce_cwe-22.html	A-TSH-CUST-280623/692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is exploited in the wild in March 2023. **CVE ID : CVE-2023-27640**		
Vendor: tsingsee					
Product: easyplayerpro					
Affected Version(s): From (including) 3.2.19.0106 Up to (including) 3.6.19.0823					
Out-of-bounds Write	05-Jun-2023	5.5	A buffer overflow in EasyPlayerPro-Win v3.2.19.0106 to v3.6.19.0823 allows attackers to cause a Denial of Service (DoS) via a crafted XML file. **CVE ID : CVE-2023-33693**	https://github.com/tsingsee/EasyPlayerPro-Win/pull/24	A-TSI-EASY-280623/693
Vendor: tsolucio					
Product: corebos					
Affected Version(s): * Up to (excluding) 8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository tsolucio/corebos prior to 8. **CVE ID : CVE-2023-3071**	https://github.com/tsolucio/corebos/commit/5e87fbc4292cf7a96fa5139ede88f4baefad104b, https://huntr.dev/bounties/3e8d5166-9bc6-46e7-94a8-cad52434a39e	A-TSO-CORE-280623/694
Vendor: txthinking					
Product: brook					
Affected Version(s): * Up to (excluding) 20230606					
Improper Neutralizat	01-Jun-2023	8.8	Brook is a cross-platform	https://github.com/txthink	A-TXT-BROO-280623/695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			programmable network tool. The `tproxy` server is vulnerable to a drive-by command injection. An attacker may fool a victim into visiting a malicious web page which will trigger requests to the local `tproxy` service leading to remote code execution. A patch is available in version 20230606. **CVE ID : CVE-2023-33965**	ing/brook/commit/314d7070c37babf6c38a0fe1eada872bb74bf03e, https://github.com/txthinking/brook/security/advisories/GHSA-vfrj-fv6p-3cpf	
Vendor: tychesoftwares					
Product: abandoned_cart_lite_for_woocommerce					
Affected Version(s): * Up to (including) 5.14.2					
Authentication Bypass Using an Alternate Path or Channel	08-Jun-2023	9.8	The Abandoned Cart Lite for WooCommerce plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 5.14.2. This is due to insufficient encryption on the user being supplied during the abandoned cart link decode through the plugin. This allows unauthenticated attackers to log in as users who have abandoned the cart, which users are typically customers. **CVE ID : CVE-2023-2986**	https://plugins.trac.wordpress.org/browser/woocommerce-abandoned-cart/trunk/woocommerce-ac.php#L1815, https://plugins.trac.wordpress.org/changeset/2922242/	A-TYC-ABAN-280623/696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: ubuntukylin					
Product: youker-assistant					
Affected Version(s): * Up to (excluding) 3.0.2-0kylin6k70-23					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Jun-2023	7.8	A vulnerability classified as critical has been found in KylinSoft youker-assistant on KylinOS. Affected is the function restore_all_sound_file. The manipulation leads to path traversal: '../filedir'. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. Upgrading to version 3.0.2-0kylin6k70-23 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-230688. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3098**	N/A	A-UBU-YOUK-280623/697
N/A	05-Jun-2023	7.1	A vulnerability classified as critical was found in KylinSoft youker-assistant on KylinOS. Affected by this vulnerability is the function delete_file	N/A	A-UBU-YOUK-280623/698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the library dbus.SystemBus of the component Arbitrary File Handler. The manipulation leads to improper access controls. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. Upgrading to version 3.0.2-0kylin6k70-23 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-230689 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3099**		
Vendor: unfocus					
Product: scripts_n_styles					
Affected Version(s): * Up to (including) 3.5.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jun-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in unFocus Projects Scripts n Styles plugin <= 3.5.7 versions. **CVE ID : CVE-2023-31236**	N/A	A-UNF-SCRI-280623/699
Vendor: urbanandroid					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: twilight					
Affected Version(s): 13.3					
N/A	09-Jun-2023	7.8	An issue found in Twilight v.13.3 for Android allows unauthorized apps to cause escalation of privilege attacks by manipulating the SharedPreference files. **CVE ID : CVE-2023-29755**	N/A	A-URB-TWIL-280623/700
Vendor: utm_tracker_project					
Product: utm_tracker					
Affected Version(s): * Up to (including) 1.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jun-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Ludwig Media UTM Tracker plugin <= 1.3.1 versions. **CVE ID : CVE-2023-23822**	N/A	A-UTM-UTM_-280623/701
Vendor: vcita					
Product: contact_form_and_calls_to_action_by_vcita					
Affected Version(s): * Up to (including) 2.6.4					
Cross-Site Request Forgery (CSRF)	03-Jun-2023	6.1	The Contact Form and Calls To Action by vcita plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.6.4. This is due to missing nonce validation in the vcita-callback.php file. This makes it possible for	https://plugins.trac.wordpress.org/browser/lead-capturing-call-to-actions-by-vcita/trunk/vcita-callback.php	A-VCI-CONT-280623/702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attackers to modify the plugin's settings and inject malicious JavaScript via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-2303**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-2023	5.4	The Contact Form and Calls To Action by vcita plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'email' parameter in versions up to, and including, 2.6.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with the edit_posts capability, such as contributors and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-2302**	https://plugins.trac.wordpress.org/browser/lead-capturing-call-to-actions-by-vcita/trunk/vcita-callback.php	A-VCI-CONT-280623/703
Product: contact_form_builder_by_vcita					
Affected Version(s): * Up to (including) 4.9.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	03-Jun-2023	6.1	The Contact Form Builder by vcita plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.9.1. This is due to missing nonce validation on the ls_parse_vcita_callback function. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious JavaScript via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-2301**	https://plugins.trac.wordpress.org/browser/contact-form-with-a-meeting-scheduler-by-vcita/trunk/system/parse_vcita_callback.php#L55	A-VCI-CONT-280623/704
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-2023	5.4	The Contact Form Builder by vcita plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'email' parameter in versions up to, and including, 4.9.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with the edit_posts capability, such as contributors and above, to inject	https://plugins.trac.wordpress.org/browser/contact-form-with-a-meeting-scheduler-by-vcita/trunk/system/parse_vcita_callback.php#L55	A-VCI-CONT-280623/705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-2300**		
Product: crm_and_lead_management_by_vcita					
Affected Version(s): * Up to (including) 2.6.2					
Cross-Site Request Forgery (CSRF)	03-Jun-2023	6.5	The CRM and Lead Management by vcita plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.6.2. This is due to missing nonce validation in the vcita-callback.php file. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious JavaScript via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-2405**	N/A	A-VCI-CRM_-280623/706
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-2023	5.4	The CRM and Lead Management by vcita plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'email' parameter in versions up to, and including, 2.6.2 due to	N/A	A-VCI-CRM_-280623/707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with the edit_posts capability, such as contributors and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-2404**		
Product: event_registration_calendar_by_vcita					
Affected Version(s): * Up to (including) 3.9.1					
Cross-Site Request Forgery (CSRF)	03-Jun-2023	6.5	The Event Registration Calendar By vcita plugin, versions up to and including 3.9.1, and Online Payments – Get Paid with PayPal, Square & Stripe plugin, for WordPress are vulnerable to Cross-Site Request Forgery. This is due to missing nonce validation in the ls_parse_vcita_callback() function. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious JavaScript via a forged request granted they can trick a site administrator into	N/A	A-VCI-EVEN-280623/708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performing an action such as clicking on a link. **CVE ID : CVE-2023-2407**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-2023	5.4	The Event Registration Calendar By vcita plugin, versions up to and including 3.9.1, and Online Payments – Get Paid with PayPal, Square & Stripe plugin, for WordPress are vulnerable to Stored Cross-Site Scripting via the 'email' parameter in versions up to, and including, 1.3.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with the edit_posts capability, such as contributors and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-2406**	N/A	A-VCI-EVEN-280623/709
Product: online_booking_\&_scheduling_calendar					
Affected Version(s): * Up to (including) 4.2.10					
Missing Authorization	09-Jun-2023	4.3	The Online Booking & Scheduling Calendar for WordPress by vcita plugin for	https://plugins.trac.wordpress.org/browser/meeting-	A-VCI-ONLI-280623/710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the vcita_save_settings_callback function in versions up to, and including, 4.2.10. This makes it possible for authenticated attackers with minimal permissions, such as a subscriber, to modify the plugins settings, upload media files, and inject malicious JavaScript. **CVE ID : CVE-2023-2414**	scheduler-by-vcita/trunk/vcita-ajax-function.php#L88	
Product: online_booking_\&_scheduling_calendar_for_wordpress					
Affected Version(s): * Up to (including) 4.2.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-2023	6.1	The Online Booking & Scheduling Calendar for WordPress by vcita plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'business_id' parameter in versions up to, and including, 4.2.10 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will	https://plugins.trac.wordpress.org/browser/meeting-scheduler-by-vcita/trunk/vcita-api-functions.php	A-VCI-ONLI-280623/711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute whenever a user accesses an injected page. **CVE ID : CVE-2023-2298**		
Missing Authorization	03-Jun-2023	5.3	The Online Booking & Scheduling Calendar for WordPress by vcita plugin for WordPress is vulnerable to unauthorized medication of data via the /wp-json/vcita-wordpress/v1/actions/auth REST-API endpoint in versions up to, and including, 4.2.10 due to a missing capability check on the processAction function. This makes it possible for unauthenticated attackers modify the plugin's settings. **CVE ID : CVE-2023-2299**	https://plugins.trac.wordpress.org/browser/meeting-scheduler-by-vcita/trunk/vcita-api-functions.php	A-VCI-ONLI-280623/712
Product: online_booking_\&_scheduling_calendar_for_wordpress_by_vcita					
Affected Version(s): * Up to (including) 4.2.10					
Cross-Site Request Forgery (CSRF)	03-Jun-2023	6.5	The Online Booking & Scheduling Calendar for WordPress by vcita plugin for WordPress is vulnerable to Cross-Site Request Forgery due to a missing nonce check on the vcita_logout_callback function in versions	N/A	A-VCI-ONLI-280623/713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			up to, and including, 4.2.10. This makes it possible for unauthenticated to logout a vctia connected account which would cause a denial of service on the appointment scheduler, via a forged request granted they can trick a site user into performing an action such as clicking on a link. **CVE ID : CVE-2023-2416**		
Missing Authorization	03-Jun-2023	5.4	The Online Booking & Scheduling Calendar for WordPress by vcita plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the vcita_logout_callback function in versions up to, and including, 4.2.10. This makes it possible for authenticated attackers with minimal permissions, such as a subscriber, to logout a vctia connected account which would cause a denial of service on the appointment scheduler.	N/A	A-VCI-ONLI-280623/714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2415		
Product: online_payments_-_get_paid_with_paypal\,_square_\&_stripe					
Affected Version(s): * Up to (including) 1.3.1					
Cross-Site Request Forgery (CSRF)	03-Jun-2023	6.5	The Event Registration Calendar By vcita plugin, versions up to and including 3.9.1, and Online Payments – Get Paid with PayPal, Square & Stripe plugin, for WordPress are vulnerable to Cross-Site Request Forgery. This is due to missing nonce validation in the ls_parse_vcita_callback() function. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious JavaScript via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-2407**	N/A	A-VCI-ONLI-280623/715
Improper Neutralization of Input During Web Page Generation	03-Jun-2023	5.4	The Event Registration Calendar By vcita plugin, versions up to and including 3.9.1, and Online Payments – Get Paid with PayPal, Square & Stripe	N/A	A-VCI-ONLI-280623/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			plugin, for WordPress are vulnerable to Stored Cross-Site Scripting via the 'email' parameter in versions up to, and including, 1.3.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with the edit_posts capability, such as contributors and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-2406**		
Vendor: vektor-inc					
Product: vk_blocks					
Affected Version(s): * Up to (including) 1.57.0.5					
N/A	03-Jun-2023	4.3	The VK Blocks plugin for WordPress is vulnerable to improper authorization via the REST 'update_vk_blocks_options' function in versions up to, and including, 1.57.0.5. This allows authenticated attackers, with contributor-level permissions or above, to change plugin	https://plugins.trac.wordpress.org/browser/vk-blocks/trunk/inc/vk-blocks/App/RestAPI/BlockMeta/class-vk-blocks-entrypoint.php	A-VEK-VK_B-280623/717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			settings including default icons. **CVE ID : CVE-2023-0583**		
N/A	03-Jun-2023	4.3	The VK Blocks plugin for WordPress is vulnerable to improper authorization via the REST 'update_options' function in versions up to, and including, 1.57.0.5. This allows authenticated attackers, with contributor-level permissions or above, to change the 'vk_font_awesome_version' option to an arbitrary value. **CVE ID : CVE-2023-0584**	https://plugins.trac.wordpress.org/browser/vk-blocks/trunk/inc/vk-blocks/font-awesome/class-vk-blocks-font-awesome-api.php	A-VEK-VK_B-280623/718
Vendor: vitejs					
Product: vite					
Affected Version(s): 2.9.15					
Use of Incorrectly-Resolved Name or Reference	01-Jun-2023	7.5	Vite provides frontend tooling. Prior to versions 2.9.16, 3.2.7, 4.0.5, 4.1.5, 4.2.3, and 4.3.9, Vite Server Options (`server.fs.deny`) can be bypassed using double forward-slash (//) allows any unauthenticated user to read file from the Vite root-path of the application including the default `fs.deny` settings (`['.env',	https://github.com/vitejs/vite/pull/13348, https://github.com/vitejs/vite/commit/813ddd6155c3d54801e264ba832d8347f6f66b32, https://github.com/vitejs/vite/security/advisories/GH	A-VIT-VITE-280623/719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'.env.*', '*.{crt,pem}']`). Only users explicitly exposing the Vite dev server to the network (using `--host` or `server.host` config option) are affected, and only files in the immediate Vite project root folder could be exposed. This issue is fixed in vite@4.3.9, vite@4.2.3, vite@4.1.5, vite@4.0.5, vite@3.2.7, and vite@2.9.16. **CVE ID : CVE-2023-34092**	SA-353f-5xf4-qw67	
Affected Version(s): From (including) 3.0.2 Up to (excluding) 3.2.7					
Use of Incorrectly-Resolved Name or Reference	01-Jun-2023	7.5	Vite provides frontend tooling. Prior to versions 2.9.16, 3.2.7, 4.0.5, 4.1.5, 4.2.3, and 4.3.9, Vite Server Options (`server.fs.deny`) can be bypassed using double forward-slash (//) allows any unauthenticated user to read file from the Vite root-path of the application including the default `fs.deny` settings (`['.env', '.env.*', '*.{crt,pem}']`). Only users explicitly exposing the Vite dev server to the network (using `--host` or `server.host` config	https://github.com/vitejs/vite/pull/13348, https://github.com/vitejs/vite/commit/813ddd6155c3d54801e264ba832d8347f6f66b32, https://github.com/vitejs/vite/security/advisories/GHSA-353f-5xf4-qw67	A-VIT-VITE-280623/720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			option) are affected, and only files in the immediate Vite project root folder could be exposed. This issue is fixed in vite@4.3.9, vite@4.2.3, vite@4.1.5, vite@4.0.5, vite@3.2.7, and vite@2.9.16. **CVE ID : CVE-2023-34092**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.5					
Use of Incorrectly-Resolved Name or Reference	01-Jun-2023	7.5	Vite provides frontend tooling. Prior to versions 2.9.16, 3.2.7, 4.0.5, 4.1.5, 4.2.3, and 4.3.9, Vite Server Options (`server.fs.deny`) can be bypassed using double forward-slash (//) allows any unauthenticated user to read file from the Vite root-path of the application including the default `fs.deny` settings (`['.env', '.env.*', '*.{crt,pem}']`). Only users explicitly exposing the Vite dev server to the network (using `--host` or `server.host` config option) are affected, and only files in the immediate Vite project root folder could be exposed. This issue is fixed in	https://github.com/vitejs/vite/pull/13348, https://github.com/vitejs/vite/commit/813ddd6155c3d54801e264ba832d8347f6f66b32, https://github.com/vitejs/vite/security/advisories/GHSA-353f-5xf4-qw67	A-VIT-VITE-280623/721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vite@4.3.9, vite@4.2.3, vite@4.1.5, vite@4.0.5, vite@3.2.7, and vite@2.9.16. **CVE ID : CVE-2023-34092**		
Affected Version(s): From (including) 4.1.0 Up to (excluding) 4.1.5					
Use of Incorrectly-Resolved Name or Reference	01-Jun-2023	7.5	Vite provides frontend tooling. Prior to versions 2.9.16, 3.2.7, 4.0.5, 4.1.5, 4.2.3, and 4.3.9, Vite Server Options (`server.fs.deny`) can be bypassed using double forward-slash (//) allows any unauthenticated user to read file from the Vite root-path of the application including the default `fs.deny` settings (`['.env', '.env.*', '*.{crt,pem}']`). Only users explicitly exposing the Vite dev server to the network (using `--host` or `server.host` config option) are affected, and only files in the immediate Vite project root folder could be exposed. This issue is fixed in vite@4.3.9, vite@4.2.3, vite@4.1.5, vite@4.0.5, vite@3.2.7, and vite@2.9.16.	https://github.com/vitejs/vite/pull/13348, https://github.com/vitejs/vite/commit/813ddd6155c3d54801e264ba832d8347f6f66b32, https://github.com/vitejs/vite/security/advisories/GHSA-353f-5xf4-qw67	A-VIT-VITE-280623/722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34092		
Affected Version(s): From (including) 4.2.0 Up to (excluding) 4.2.3					
Use of Incorrectly-Resolved Name or Reference	01-Jun-2023	7.5	Vite provides frontend tooling. Prior to versions 2.9.16, 3.2.7, 4.0.5, 4.1.5, 4.2.3, and 4.3.9, Vite Server Options (`server.fs.deny`) can be bypassed using double forward-slash (//) allows any unauthenticated user to read file from the Vite root-path of the application including the default `fs.deny` settings (`['.env', '.env.*', '*.{crt,pem}']`). Only users explicitly exposing the Vite dev server to the network (using `--host` or `server.host` config option) are affected, and only files in the immediate Vite project root folder could be exposed. This issue is fixed in vite@4.3.9, vite@4.2.3, vite@4.1.5, vite@4.0.5, vite@3.2.7, and vite@2.9.16. **CVE ID : CVE-2023-34092**	https://github.com/vitejs/vite/pull/13348, https://github.com/vitejs/vite/commit/813ddd6155c3d54801e264ba832d8347f6f66b32, https://github.com/vitejs/vite/security/advisories/GHSA-353f-5xf4-qw67	A-VIT-VITE-280623/723
Affected Version(s): From (including) 4.3.0 Up to (excluding) 4.3.9					
Use of Incorrectly	01-Jun-2023	7.5	Vite provides frontend tooling. Prior to	https://github.com/vitejs/	A-VIT-VITE-280623/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
-Resolved Name or Reference			versions 2.9.16, 3.2.7, 4.0.5, 4.1.5, 4.2.3, and 4.3.9, Vite Server Options (`server.fs.deny`) can be bypassed using double forward-slash (//) allows any unauthenticated user to read file from the Vite root-path of the application including the default `fs.deny` settings (`['.env', '.env.*', '*.{crt,pem}']`). Only users explicitly exposing the Vite dev server to the network (using `--host` or `server.host` config option) are affected, and only files in the immediate Vite project root folder could be exposed. This issue is fixed in vite@4.3.9, vite@4.2.3, vite@4.1.5, vite@4.0.5, vite@3.2.7, and vite@2.9.16. **CVE ID : CVE-2023-34092**	vite/pull/13348, https://github.com/vitejs/vite/commit/813ddd6155c3d54801e264ba832d8347f6f66b32, https://github.com/vitejs/vite/security/advisories/GHSA-353f-5xf4-qw67	
Vendor: Vmware					
Product: vrealize_network_insight					
Affected Version(s): From (including) 6.2.0 Up to (including) 6.10.0					
Improper Neutralization of Special Elements	07-Jun-2023	9.8	Aria Operations for Networks contains a command injection vulnerability. A malicious actor with	https://www.vmware.com/security/advisories/VMSA-	A-VMW-VREA-280623/725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			network access to VMware Aria Operations for Networks may be able to perform a command injection attack resulting in remote code execution. **CVE ID : CVE-2023-20887**	2023-0012.html	
Deserialization of Untrusted Data	07-Jun-2023	8.8	Aria Operations for Networks contains an authenticated deserialization vulnerability. A malicious actor with network access to VMware Aria Operations for Networks and valid 'member' role credentials may be able to perform a deserialization attack resulting in remote code execution. **CVE ID : CVE-2023-20888**	https://www.vmware.com/security/advisories/VMSA-2023-0012.html	A-VMW-VREA-280623/726
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jun-2023	7.5	Aria Operations for Networks contains an information disclosure vulnerability. A malicious actor with network access to VMware Aria Operations for Networks may be able to perform a command injection attack resulting in	https://www.vmware.com/security/advisories/VMSA-2023-0012.html	A-VMW-VREA-280623/727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2023-20889**		
Vendor: wclovers					
Product: woocommerce_multivendor_marketplace					
Affected Version(s): * Up to (including) 1.5.3					
Missing Authorization	09-Jun-2023	5.4	The WooCommerce Multivendor Marketplace – REST API plugin for WordPress is vulnerable to unauthorized access of data and addition of data due to a missing capability check on the 'get_item', 'get_order_notes' and 'add_order_note' functions in versions up to, and including, 1.5.3. This makes it possible for authenticated attackers with subscriber privileges or above, to view the order details and order notes, and add order notes. **CVE ID : CVE-2023-2275**	https://plugins.trac.wordpress.org/browser/wcfm-marketplace-rest-api/tags/1.5.3/includes/api/class-api-order-controller.php#L167, https://plugins.trac.wordpress.org/changeset/2904331/	A-WCL-WOOC-280623/728
Vendor: wddgroup					
Product: fantasy					
Affected Version(s): 2.1.8					
Unrestricted Upload of File with	02-Jun-2023	8.8	Wade Graphic Design FANTSY has a vulnerability of insufficient filtering for file type in its file	N/A	A-WDD-FANT-280623/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			update function. An authenticated remote attacker with general user privilege can exploit this vulnerability to upload a PHP file containing a webshell to perform arbitrary system operation or disrupt service. **CVE ID : CVE-2023-28699**		
Product: fantsy					
Affected Version(s): 2.1.8					
Incorrect Authorization	02-Jun-2023	9.8	Wade Graphic Design FANTSY has a vulnerability of insufficient authorization check. An unauthenticated remote user can exploit this vulnerability by modifying URL parameters to gain administrator privileges to perform arbitrary system operation or disrupt service. **CVE ID : CVE-2023-28698**	N/A	A-WDD-FANT-280623/730
Vendor: weavertheme					
Product: weaver_show_posts					
Affected Version(s): * Up to (including) 1.6					
Improper Neutralization of Input During	09-Jun-2023	5.4	The Weaver Show Posts Plugin for WordPress is vulnerable to stored Cross-Site Scripting	https://plugins.trac.wordpress.org/browser/show-posts/tags/1.	A-WEA-WEAV-280623/731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			due to insufficient escaping of the profile display name in versions up to, and including, 1.6. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-1404**	6/includes/atw-showposts-sc.php#L368	
Product: weaver_xtreme_theme					
Affected Version(s): * Up to (including) 5.0.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	5.4	The Weaver Xtreme Theme for WordPress is vulnerable to stored Cross-Site Scripting due to insufficient escaping of the profile display name in versions up to, and including, 5.0.7. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-1403**	https://themes.trac.wordpress.org/browser/weaver-xtreme/5.0.7/includes/lib-content.php#L1081	A-WEA-WEAV-280623/732
Vendor: webbax					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: king-avis					
Affected Version(s): * Up to (excluding) 17.3.15					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Jun-2023	4.9	Improper Limitation of a Pathname leads to a Path Traversal vulnerability in the module King-Avis for Prestashop, allowing a user knowing the download token to read arbitrary local files.This issue affects King-Avis: before 17.3.15. **CVE ID : CVE-2023-3031**	N/A	A-WEB-KING-280623/733
Vendor: webfactoryltd					
Product: under_construction					
Affected Version(s): * Up to (including) 3.96					
Cross-Site Request Forgery (CSRF)	09-Jun-2023	4.3	The Under Construction plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.96. This is due to missing or incorrect nonce validation on the dismiss_notice function called via the admin_action_ucp_dismiss_notice action. This makes it possible for unauthenticated attackers to dismiss plugin notifications via a forged request granted they can trick	https://plugins.trac.wordpress.org/browser/under-construction-page/trunk/under-construction.php?rev=2848705#L901	A-WEB-UNDE-280623/734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-0831**		
Cross-Site Request Forgery (CSRF)	09-Jun-2023	4.3	The Under Construction plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.96. This is due to missing or incorrect nonce validation on the install_weglot function called via the admin_action_install_weglot action. This makes it possible for unauthenticated attackers to perform an unauthorized install of the Weglot Translate plugin via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-0832**	https://plugins.trac.wordpress.org/browser/under-construction-page/trunk/under-construction.php?rev=2848705#L2389	A-WEB-UNDE-280623/735
Vendor: webwizards					
Product: b2bking					
Affected Version(s): * Up to (including) 4.6.00					
N/A	07-Jun-2023	6.5	The B2BKing plugin for WordPress is vulnerable to unauthorized modification of data	N/A	A-WEB-B2BK-280623/736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to a missing capability check on the 'b2bking_save_price_import' function in versions up to, and including, 4.6.00. This makes it possible for Authenticated attackers with subscriber or customer-level permissions to modify the pricing of any product on the site. **CVE ID : CVE-2023-3125**		
N/A	07-Jun-2023	4.3	The B2BKing plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'b2bkingdownloadpricelist' function in versions up to, and including, 4.6.00. This makes it possible for Authenticated attackers with subscriber or customer-level permissions to retrieve the full pricing list of all products on the site. **CVE ID : CVE-2023-3126**	N/A	A-WEB-B2BK-280623/737
Vendor: wickedplugins					
Product: wicked_folders					
Affected Version(s): * Up to (including) 2.18.16					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	09-Jun-2023	4.3	The Wicked Folders plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.18.16. This is due to missing or incorrect nonce validation on the ajax_save_sort_order function. This makes it possible for unauthenticated attackers to invoke this function via forged request granted they can trick a site administrator into performing an action such as clicking on a link leading them to perform actions intended for administrators such as changing the folder structure maintained by the plugin. **CVE ID : CVE-2023-0729**	https://plugins.trac.wordpress.org/browser/wicked-folders/tags/2.18.16/lib/class-wicked-folders-ajax.php	A-WIC-WICK-280623/738
Vendor: Wireshark					
Product: wireshark					
Affected Version(s): * Up to (excluding) 3.6.14					
Out-of-bounds Write	07-Jun-2023	9.8	Due to failure in validating the length provided by an attacker-crafted MSMMS packet, Wireshark version 4.0.5 and prior, in an unusual configuration, is susceptible to a heap-based buffer	N/A	A-WIR-WIRE-280623/739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow, and possibly code execution in the context of the process running Wireshark **CVE ID : CVE-2023-0667**		
Affected Version(s): From (including) 3.6.0 Up to (excluding) 3.6.14					
Out-of-bounds Write	07-Jun-2023	6.5	Due to failure in validating the length provided by an attacker-crafted IEEE-C37.118 packet, Wireshark version 4.0.5 and prior, by default, is susceptible to a heap-based buffer overflow, and possibly code execution in the context of the process running Wireshark. **CVE ID : CVE-2023-0668**	https://www.wireshark.org/security/wnpa-sec-2023-19.html	A-WIR-WIRE-280623/740
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.6					
Out-of-bounds Write	07-Jun-2023	9.8	Due to failure in validating the length provided by an attacker-crafted MSMMS packet, Wireshark version 4.0.5 and prior, in an unusual configuration, is susceptible to a heap-based buffer overflow, and possibly code execution in the context of the process running Wireshark **CVE ID : CVE-2023-0667**	N/A	A-WIR-WIRE-280623/741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Jun-2023	6.5	Due to failure in validating the length provided by an attacker-crafted RTPS packet, Wireshark version 4.0.5 and prior, by default, is susceptible to a heap-based buffer overflow, and possibly code execution in the context of the process running Wireshark. **CVE ID : CVE-2023-0666**	https://www.wireshark.org/security/wnpa-sec-2023-18.html	A-WIR-WIRE-280623/742
Out-of-bounds Write	07-Jun-2023	6.5	Due to failure in validating the length provided by an attacker-crafted IEEE-C37.118 packet, Wireshark version 4.0.5 and prior, by default, is susceptible to a heap-based buffer overflow, and possibly code execution in the context of the process running Wireshark. **CVE ID : CVE-2023-0668**	https://www.wireshark.org/security/wnpa-sec-2023-19.html	A-WIR-WIRE-280623/743
Vendor: wisetr					
Product: user_email_verification_for_woocommerce					
Affected Version(s): * Up to (including) 3.5.0					
Missing Authentication for Critical Function	03-Jun-2023	9.8	The User Email Verification for WooCommerce plugin for WordPress is vulnerable to authentication bypass via authenticate_user_by_email in versions up	https://plugins.trac.wordpress.org/browser/woo-confirmation-email/tags/3.5.0/public/class-xlwuev-woocommerc	A-WIS-USER-280623/744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to, and including, 3.5.0. This is due to a random token generation weakness in the resend_verification_email function. This allows unauthenticated attackers to impersonate users and trigger an email address verification for arbitrary accounts, including administrative accounts, and automatically be logged in as that user, including any site administrators. This requires the Allow Automatic Login After Successful Verification setting to be enabled, which it is not by default. **CVE ID : CVE-2023-2781**	e-confirmation-email-public.php#L506	
Vendor: wpdevart					
Product: pricing_table_builder					
Affected Version(s): * Up to (including) 1.1.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jun-2023	7.2	The Pricing Table Builder WordPress plugin through 1.1.6 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high-	N/A	A-WPD-PRIC-280623/745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege users such as admins. **CVE ID : CVE-2023-0900**		
Vendor: wpdeveloper					
Product: essential_blocks					
Affected Version(s): * Up to (including) 4.0.6					
Missing Authorization	09-Jun-2023	4.3	The Essential Blocks plugin for WordPress is vulnerable to unauthorized use of functionality due to a missing capability check on the save function in versions up to, and including, 4.0.6. This makes it possible for subscriber-level attackers to save plugin settings. While a nonce check is present, it is only executed when a nonce is provided. Not providing a nonce results in the nonce verification to be skipped. There is no capability check. **CVE ID : CVE-2023-2083**	https://plugins.trac.wordpress.org/browser/essential-blocks/tags/4.0.6/includes/Admin/Admin.php	A-WPD-ESSE-280623/746
Missing Authorization	09-Jun-2023	4.3	The Essential Blocks plugin for WordPress is vulnerable to unauthorized use of functionality due to a missing capability check on the get function in versions up to, and including, 4.0.6. This makes it	https://plugins.trac.wordpress.org/browser/essential-blocks/tags/4.0.6/includes/Admin/Admin.php	A-WPD-ESSE-280623/747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible for subscriber-level attackers to obtain plugin settings. While a nonce check is present, it is only executed when a nonce is provided. Not providing a nonce results in the nonce verification to be skipped. There is no capability check. **CVE ID : CVE-2023-2084**		
Missing Authorization	09-Jun-2023	4.3	The Essential Blocks plugin for WordPress is vulnerable to unauthorized use of functionality due to a missing capability check on the templates function in versions up to, and including, 4.0.6. This makes it possible for subscriber-level attackers to obtain plugin template information. While a nonce check is present, it is only executed when a nonce is provided. Not providing a nonce results in the nonce verification to be skipped. There is no capability check. **CVE ID : CVE-2023-2085**	https://plugins.trac.wordpress.org/browser/essential-blocks/tags/4.0.6/includes/Admin/Admin.php	A-WPD-ESSE-280623/748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	09-Jun-2023	4.3	The Essential Blocks plugin for WordPress is vulnerable to unauthorized use of functionality due to a missing capability check on the template_count function in versions up to, and including, 4.0.6. This makes it possible for subscriber-level attackers to obtain plugin template information. While a nonce check is present, it is only executed when a nonce is provided. Not providing a nonce results in the nonce verification to be skipped. There is no capability check. **CVE ID : CVE-2023-2086**	https://plugins.trac.wordpress.org/browser/essential-blocks/tags/4.0.6/includes/Admin/Admin.php	A-WPD-ESSE-280623/749
Cross-Site Request Forgery (CSRF)	09-Jun-2023	4.3	The Essential Blocks plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.0.6. This is due to missing or incorrect nonce validation on the save function. This makes it possible for unauthenticated attackers to change plugin settings via a forged request granted they can trick	https://plugins.trac.wordpress.org/browser/essential-blocks/tags/4.0.6/includes/Admin/Admin.php	A-WPD-ESSE-280623/750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-2087**		
Product: reviewx					
Affected Version(s): * Up to (including) 1.6.13					
Improper Privilege Management	06-Jun-2023	8.8	The ReviewX plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 1.6.13 due to insufficient restriction on the 'rx_set_screen_options' function. This makes it possible for authenticated attackers, with minimal permissions such as a subscriber, to modify their user role by supplying the 'wp_screen_options[option]' and 'wp_screen_options[value]' parameters during a screen option update. **CVE ID : CVE-2023-2833**	N/A	A-WPD-REVI-280623/751
Vendor: wpdirectorykit					
Product: wp_directory_kit					
Affected Version(s): * Up to (excluding) 1.2.3					
Missing Authorization	09-Jun-2023	5.3	The WP Directory Kit plugin for WordPress is vulnerable to unauthorized modification of data	https://plugins.trac.wordpress.org/changeset/2907164/,	A-WPD-WP_D-280623/752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and loss of data due to a missing capability check on the 'ajax_public' function in versions up to, and including, 1.2.2. This makes it possible for unauthenticated attackers to delete or change plugin settings, import demo data, delete Directory Kit related posts and terms, and install arbitrary plugins. A partial patch was introduced in version 1.2.0 and an additional partial patch was introduced in version 1.2.2, but the issue was not fully patched until 1.2.3. **CVE ID : CVE-2023-2280**	https://plugins.trac.wordpress.org/browser/wpdirectorykit/tags/1.1.8/public/class-wpdirectorykit-public.php#L249	
Affected Version(s): * Up to (including) 1.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jun-2023	6.1	The WP Directory Kit plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'search' parameter in versions up to, and including, 1.2.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully	https://www.wordfence.com/threat-intel/vulnerabilities/id/847f1c00-0e8f-4d38-84af-fe959e2efe5c?source=cve, https://plugins.trac.wordpress.org/changeset/2917413/wpdirectorykit/trunk/application/views	A-WPD-WP_D-280623/753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2023-2835**	/wdk_messages/index.php	
Vendor: wpdownloadmanager					
Product: wordpress_download_manager					
Affected Version(s): * Up to (excluding) 3.2.71					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	5.4	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpdm_members', 'wpdm_login_form', 'wpdm_reg_form' shortcodes in versions up to, and including, 3.2.70 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-2305**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2906403%40download-manager&new=2906403%40download-manager&sfp_email=&sfph_mail=	A-WPD-WORD-280623/754
Vendor: Wpeasycart					
Product: wp_easycart					
Affected Version(s): * Up to (including) 5.4.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	09-Jun-2023	4.3	The WP EasyCart plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 5.4.8. This is due to missing or incorrect nonce validation on the process_delete_product function. This makes it possible for unauthenticated attackers to delete products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-2891**	https://plugins.trac.wordpress.org/changeset/2917958/wp-easycart	A-WPE-WP_E-280623/755
Cross-Site Request Forgery (CSRF)	09-Jun-2023	4.3	The WP EasyCart plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 5.4.8. This is due to missing or incorrect nonce validation on the process_bulk_delete_product function. This makes it possible for unauthenticated attackers to bulk delete products via a forged request granted they can trick a site administrator into performing an	https://plugins.trac.wordpress.org/changeset/2917958/wp-easycart	A-WPE-WP_E-280623/756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action such as clicking on a link. **CVE ID : CVE-2023-2892**		
Cross-Site Request Forgery (CSRF)	09-Jun-2023	4.3	The WP EasyCart plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 5.4.8. This is due to missing or incorrect nonce validation on the process_deactivate_product function. This makes it possible for unauthenticated attackers to deactivate products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-2893**	https://plugins.trac.wordpress.org/changeset/2917958/wp-easycart	A-WPE-WP_E-280623/757
Cross-Site Request Forgery (CSRF)	09-Jun-2023	4.3	The WP EasyCart plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 5.4.8. This is due to missing or incorrect nonce validation on the process_bulk_deactivate_product function. This makes it possible for unauthenticated attackers to bulk deactivate products via a forged request	https://plugins.trac.wordpress.org/changeset/2917958/wp-easycart	A-WPE-WP_E-280623/758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-2894**		
Cross-Site Request Forgery (CSRF)	09-Jun-2023	4.3	The WP EasyCart plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 5.4.8. This is due to missing or incorrect nonce validation on the process_bulk_activate_product function. This makes it possible for unauthenticated attackers to bulk activate products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-2895**	https://plugins.trac.wordpress.org/changeset/2917958/wp-easycart	A-WPE-WP_E-280623/759
Cross-Site Request Forgery (CSRF)	09-Jun-2023	4.3	The WP EasyCart plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 5.4.8. This is due to missing or incorrect nonce validation on the process_duplicate_product function. This makes it possible for unauthenticated	https://plugins.trac.wordpress.org/changeset/2917958/wp-easycart	A-WPE-WP_E-280623/760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to duplicate products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-2896**		
Vendor: wpexperts					
Product: wp_multi_store_locator					
Affected Version(s): * Up to (including) 2.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2023	5.4	The WP Multi Store Locator WordPress plugin through 2.4 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-0152**	N/A	A-WPE-WP_M-280623/761
Vendor: wpfastestcache					
Product: wp_fastest_cache					
Affected Version(s): * Up to (including) 1.1.2					
Missing Authorization	09-Jun-2023	4.3	The WP Fastest Cache plugin for WordPress is vulnerable to unauthorized cache deletion in versions up to, and including, 1.1.2 due to a missing	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=289315	A-WPF-WP_F-280623/762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			capability check in the deleteCacheToolbar function . This makes it possible for authenticated attackers, with subscriber-level permissions and above, to delete the site's cache. **CVE ID : CVE-2023-1375**	8%40wp-fastest-cache&new=2893158%40wp-fastest-cache&sfp_email=&sfph_mail=, https://plugins.trac.wordpress.org/browser/wp-fastest-cache/trunk/wpFastestCache.php#L866	
Vendor: wpmanageninja					
Product: fluentcrm					
Affected Version(s): * Up to (including) 2.7.40					
Use of a One-Way Hash without a Salt	09-Jun-2023	3.7	The FluentCRM - Marketing Automation For WordPress plugin for WordPress is vulnerable to unauthorized modification of data in versions up to, and including, 2.7.40 due to the use of an MD5 hash without a salt to control subscriptions. This makes it possible for unauthenticated attackers to unsubscribe users from lists and manage subscriptions, granted they gain access to any targeted subscribers email address. **CVE ID : CVE-2023-1430**	https://plugins.trac.wordpress.org/changeset/2899218/fluent-crm/tags/2.8.0/app/Hooks/Handlers/ExternalPages.php?old=2873074&old_path=fluent-crm%2Ftags%2F2.7.40%2Fapp%2FHooks%2FHandlers%2FExternalPages.php	A-WPM-FLUE-280623/763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: wpmet					
Product: metform_elementor_contact_form_builder					
Affected Version(s): * Up to (including) 3.3.0					
Improper Neutralization of Formula Elements in a CSV File	09-Jun-2023	7.8	The Metform Elementor Contact Form Builder plugin for WordPress is vulnerable to CSV injection in versions up to, and including, 3.3.0. This allows unauthenticated attackers to embed untrusted input into exported CSV files, which can result in code execution when these files are downloaded and opened on a local system with a vulnerable configuration. **CVE ID : CVE-2023-0721**	https://plugins.trac.wordpress.org/changeset/2907471/, https://plugins.trac.wordpress.org/browser/metform/trunk/core/entries/export.php?rev=2845078	A-WPM-METF-280623/764
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	5.4	The Metform Elementor Contact Form Builder for WordPress is vulnerable to Cross-Site Scripting by using the 'mf' shortcode to echo unescaped form submissions in versions up to, and including, 3.3.0. This allows authenticated attackers, with contributor-level permissions or above, to inject arbitrary web scripts in pages that	https://plugins.trac.wordpress.org/browser/metform/trunk/base/shortcode.php?rev=2845078	A-WPM-METF-280623/765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			will execute when the victim visits a specific link. Note that getting the JavaScript to execute still requires user interaction as the victim must visit a crafted link with the form entry id, but the script itself is stored in the site database. **CVE ID : CVE-2023-0695**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	5.4	The Metform Elementor Contact Form Builder for WordPress is vulnerable to Cross-Site Scripting by using the 'mf_first_name' shortcode to echo unescaped form submissions in versions up to, and including, 3.3.0. This allows authenticated attackers, with contributor-level permissions or above, to inject arbitrary web scripts in pages that will execute when the victim visits a a page containing the shortcode when the submission id is present in the query string. Note that getting the JavaScript to execute requires user interaction as the victim must visit a crafted link with the	https://plugins.trac.wordpress.org/changeset/2907471/, https://plugins.trac.wordpress.org/browser/metform/trunk/base/shortcode.php?rev=2845078	A-WPM-METF-280623/766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			form entry id, but the script itself is stored in the site database. **CVE ID : CVE-2023-0708**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	5.4	The Metform Elementor Contact Form Builder for WordPress is vulnerable to Cross-Site Scripting by using the 'mf_last_name' shortcode to echo unescaped form submissions in versions up to, and including, 3.3.0. This allows authenticated attackers, with contributor-level permissions or above, to inject arbitrary web scripts in pages that will execute when the victim visits a a page containing the shortcode when the submission id is present in the query string. Note that getting the JavaScript to execute requires user interaction as the victim must visit a crafted link with the form entry id, but the script itself is stored in the site database. **CVE ID : CVE-2023-0709**	https://plugins.trac.wordpress.org/changeset/2907471/, https://plugins.trac.wordpress.org/browser/metform/trunk/base/shortcode.php?rev=2845078	A-WPM-METF-280623/767
Improper Neutralization of	09-Jun-2023	5.4	The Metform Elementor Contact Form Builder for	https://plugins.trac.wordpress.org/brows	A-WPM-METF-280623/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			WordPress is vulnerable to Cross-Site Scripting by using the 'fname' attribute of the 'mf_thankyou' shortcode to echo unescaped form submissions in versions up to, and including, 3.3.0. This allows authenticated attackers, with contributor-level permissions or above, to inject arbitrary web scripts in pages that will execute when the victim visits a a page containing the shortcode when the submission id is present in the query string. Note that getting the JavaScript to execute requires user interaction as the victim must visit a crafted link with the form entry id, but the script itself is stored in the site database. Additionally this requires successful payment, increasing the complexity. **CVE ID : CVE-2023-0710**	er/metform/trunk/base/shortcode.php?rev=2845078	
Missing Authorization	09-Jun-2023	5.3	The Metform Elementor Contact Form Builder plugin for WordPress is vulnerable to unauthorized	https://plugins.trac.wordpress.org/changeset/2907471/, https://plugin	A-WPM-METF-280623/769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permalink structure update due to a missing capability check on the permalink_setup function in versions up to, and including, 3.3.0. This makes it possible for unauthenticated attackers to change the permalink structure. **CVE ID : CVE-2023-1843**	s.trac.wordpress.org/browser/metform/trunk/plugin.php#L544	
Affected Version(s): * Up to (including) 3.3.1					
Authorization Bypass Through User-Controlled Key	09-Jun-2023	6.5	The Metform Elementor Contact Form Builder for WordPress is vulnerable to Information Disclosure via the 'mf_thankyou' shortcode in versions up to, and including, 3.3.1. This allows authenticated attackers, with subscriber-level capabilities or above to obtain sensitive information about form submissions, including payment status, and transaction ID. **CVE ID : CVE-2023-0688**	https://plugins.trac.wordpress.org/browser/metform/trunk/base/shortcode.php?rev=2845078, https://plugins.trac.wordpress.org/changeset/2910040/	A-WPM-METF-280623/770
Authorization Bypass Through	09-Jun-2023	4.3	The Metform Elementor Contact Form Builder for	https://plugins.trac.wordpress.org/brows	A-WPM-METF-280623/771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
User-Controlled Key			WordPress is vulnerable to Information Disclosure via the 'mf_last_name' shortcode in versions up to, and including, 3.3.1. This allows authenticated attackers, with subscriber-level capabilities or above to obtain sensitive information about arbitrary form submissions, specifically the submitter's last name. **CVE ID : CVE-2023-0691**	er/metform/trunk/base/shortcode.php?rev=2845078, https://plugins.trac.wordpress.org/changeset/2910040/	
Authorization Bypass Through User-Controlled Key	09-Jun-2023	4.3	The Metform Elementor Contact Form Builder for WordPress is vulnerable to Information Disclosure via the 'mf_payment_status' shortcode in versions up to, and including, 3.3.1. This allows authenticated attackers, with subscriber-level capabilities or above to obtain sensitive information about the payment status of arbitrary form submissions. **CVE ID : CVE-2023-0692**	https://plugins.trac.wordpress.org/browser/metform/trunk/base/shortcode.php?rev=2845078, https://plugins.trac.wordpress.org/changeset/2910040/	A-WPM-METF-280623/772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authorization Bypass Through User-Controlled Key	09-Jun-2023	4.3	The Metform Elementor Contact Form Builder for WordPress is vulnerable to Information Disclosure via the 'mf_transaction_id' shortcode in versions up to, and including, 3.3.1. This allows authenticated attackers, with subscriber-level capabilities or above to obtain sensitive information about the transaction ids of arbitrary form submissions that included payment. **CVE ID : CVE-2023-0693**	https://plugins.trac.wordpress.org/browser/metform/trunk/base/shortcode.php?rev=2845078, https://plugins.trac.wordpress.org/changeset/2910040/	A-WPM-METF-280623/773
Authorization Bypass Through User-Controlled Key	09-Jun-2023	4.3	The Metform Elementor Contact Form Builder for WordPress is vulnerable to Information Disclosure via the 'mf' shortcode in versions up to, and including, 3.3.1. This allows authenticated attackers, with subscriber-level capabilities or above to obtain sensitive information about any standard form field of any form submission. **CVE ID : CVE-2023-0694**	https://plugins.trac.wordpress.org/browser/metform/trunk/base/shortcode.php?rev=2845078, https://plugins.trac.wordpress.org/changeset/2910040/	A-WPM-METF-280623/774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: wpoperation					
Product: salert_-_fake_sales_notification_woocommerce					
Affected Version(s): * Up to (including) 1.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jun-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WPoperation SALERT – Fake Sales Notification WooCommerce plugin <= 1.2.1 versions. **CVE ID : CVE-2023-32118**	N/A	A-WPO-SALE-280623/775
Vendor: wpwax					
Product: directorist					
Affected Version(s): * Up to (including) 7.5.4					
Improper Input Validation	09-Jun-2023	8.8	The Directorist plugin for WordPress is vulnerable to an arbitrary user password reset in versions up to, and including, 7.5.4. This is due to a lack of validation checks within login.php. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to reset the password of an arbitrary user and gain elevated (e.g., administrator) privileges. **CVE ID : CVE-2023-1888**	N/A	A-WPW-DIRE-280623/776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authorization Bypass Through User-Controlled Key	09-Jun-2023	6.5	The Directorist plugin for WordPress is vulnerable to an Insecure Direct Object Reference in versions up to, and including, 7.5.4. This is due to improper validation and authorization checks within the listing_task function. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to delete arbitrary posts. **CVE ID : CVE-2023-1889**	N/A	A-WPW-DIRE-280623/777
Vendor: wpwhitesecurity					
Product: wp_activity_log					
Affected Version(s): * Up to (including) 4.5.0					
Missing Authorization	09-Jun-2023	4.3	The WP Activity Log plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the handle_ajax_call function in versions up to, and including, 4.5.0. This makes it possible for authenticated attackers, with subscriber-level access or higher, to obtain a list of users with accounts on the site. This includes ids, usernames and emails.	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2911239%40wp-security-audit-log%2Ftrunk&old=2897171%40wp-security-audit-log%2Ftrunk&sfp_email=&sfph_mail=	A-WPW-WP_A-280623/778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2261		
Missing Authorization	09-Jun-2023	4.3	The WP Activity Log Premium plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ajax_switch_db function in versions up to, and including, 4.5.0. This makes it possible for authenticated attackers with subscriber-level or higher to make changes to the plugin's settings. **CVE ID : CVE-2023-2284**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2911239%40wp-security-audit-log%2Ftrunk&old=2897171%40wp-security-audit-log%2Ftrunk&sfp_email=&sfph_mail=	A-WPW-WP_A-280623/779
Cross-Site Request Forgery (CSRF)	09-Jun-2023	4.3	The WP Activity Log Premium plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.5.0. This is due to missing or incorrect nonce validation on the ajax_switch_db function. This makes it possible for unauthenticated attackers to make changes to the plugin's settings via a forged request granted they can trick a site administrator	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2911239%40wp-security-audit-log%2Ftrunk&old=2897171%40wp-security-audit-log%2Ftrunk&sfp_email=&sfph_mail=	A-WPW-WP_A-280623/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into performing an action such as clicking on a link. **CVE ID : CVE-2023-2285**		
Cross-Site Request Forgery (CSRF)	09-Jun-2023	4.3	The WP Activity Log for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.5.0. This is due to missing or incorrect nonce validation on the ajax_run_cleanup function. This makes it possible for unauthenticated attackers to invoke this function via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-2286**	https://plugins.trac.wordpress.org/browser/wp-security-audit-log/trunk/classes/Views/Settings.php#L278	A-WPW-WP_A-280623/781
Vendor: wp_abstracts_project					
Product: wp_abstracts					
Affected Version(s): * Up to (including) 2.6.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jun-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Kevon Adonis WP Abstracts plugin <= 2.6.2 versions. **CVE ID : CVE-2023-29385**	N/A	A-WP_-WP_A-280623/782
Vendor: wp_user_switch_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wp_user_switch					
Affected Version(s): * Up to (including) 1.0.2					
Authentication Bypass Using an Alternate Path or Channel	06-Jun-2023	8.8	The WP User Switch plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 1.0.2. This is due to incorrect authentication checking in the 'wpus_allow_user_to_admin_bar_menu' function with the 'wpus_who_switch' cookie value. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to log in as any existing user on the site, such as an administrator, if they have access to the username. **CVE ID : CVE-2023-2546**	https://www.wordfence.com/threat-intel/vulnerabilities/id/e89d912d-fa7a-4fb1-8872-95fa861c21ca?source=cve, https://plugins.trac.wordpress.org/changeset/2921182/wp-user-switch/trunk/inc/functions.php	A-WP_-WP_U-280623/783
Vendor: x-wrt					
Product: luci					
Affected Version(s): * Up to (excluding) 22.10_b202303121313					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jun-2023	6.1	A vulnerability, which was classified as problematic, has been found in X-WRT luci up to 22.10_b202303061504. This issue affects the function run_action of the file modules/luci-	https://github.com/x-wrt/luci/commit/24d7da2416b9ab246825c33c213fe939a89b369c	A-X-W-LUCI-280623/784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			base/ucode/dispatcher.uc of the component 404 Error Template Handler. The manipulation of the argument request_path leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 22.10_b20230312131 3 is able to address this issue. The name of the patch is 24d7da2416b9ab246 825c33c213fe939a89 b369c. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-230663. **CVE ID : CVE-2023-3085**		
Vendor: xml_library_project					
Product: xml_library					
Affected Version(s): * Up to (excluding) 0.8.14					
Improper Restriction of XML External Entity Reference	05-Jun-2023	7.5	The xml-rs crate before 0.8.14 for Rust and Crab allows a denial of service (panic) via an invalid <! token (such as <!DOCTYPEs/%<!A nesting) in an XML document. The earliest affected version is 0.8.9. **CVE ID : CVE-2023-34411**	https://github.com/netvl/xml-rs/commit/c09549a187e62d39d40467f129e64abf32efc35c, https://github.com/00xc/xml-rs/commit/0f084d45aa53e	A-XML-XML_-280623/785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				4a27476961785f59f2bd7d59a9f, https://github.com/netvl/xml-rs/compare/0.8.13...0.8.14	
Vendor: xpdfreader					
Product: xpdf					
Affected Version(s): * Up to (excluding) 4.05					
Divide By Zero	02-Jun-2023	3.3	An excessively large PDF page size (found in fuzz testing, unlikely in normal PDF files) can result in a divide-by-zero in Xpdf's text extraction code. This is related to CVE-2022-30524, but the problem here is caused by a very large page size, rather than by a very large character coordinate. **CVE ID : CVE-2023-3044**	https://www.xpdfreader.com/security-bug/CVE-2023-3044.html	A-XPD-XPDF-280623/786
Vendor: xxl-rpc_project					
Product: xxl-rpc					
Affected Version(s): * Up to (including) 1.7.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	07-Jun-2023	9.8	xxl-rpc v1.7.0 was discovered to contain a deserialization vulnerability via the component com.xxl.rpc.core.remoting.net.impl.netty.codec.NettyDecode#decode. **CVE ID : CVE-2023-33496**	N/A	A-XXL-XXL--280623/787
Vendor: yajl_project					
Product: yajl					
Affected Version(s): 2.1.0					
Missing Release of Memory after Effective Lifetime	06-Jun-2023	6.5	There's a memory leak in yajl 2.1.0 with use of yajl_tree_parse function. which will cause out-of-memory in server and cause crash. **CVE ID : CVE-2023-33460**	https://github.com/lloyd/yajl/issues/250	A-YAJ-YAJL-280623/788
Vendor: yudiz					
Product: wp_replicate_post					
Affected Version(s): * Up to (including) 4.0.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Jun-2023	8.8	The WP Replicate Post plugin for WordPress is vulnerable to SQL Injection via the post_id parameter in versions up to, and including, 4.0.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for contributor-level	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2910474%40wp-replicate-post%2Ftrunk&old=2896518%40wp-replicate-post%2Ftrunk&sfp_email=	A-YUD-WP_R-280623/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers or higher to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-2237**	&sfph_mail=#file3	
Vendor: zxcvbn-ts_project					
Product: zxcvbn-ts					
Affected Version(s): * Up to (excluding) 3.0.2					
Uncontrolled Resource Consumption	07-Jun-2023	7.5	zxcvbn-ts is an open source password strength estimator written in typescript. This vulnerability affects users running on the nodeJS platform which are using the second argument of the zxcvbn function. It can result in an unbounded resource consumption as the user inputs array is extended with every function call. Browsers are impacted, too but a single user need to do a lot of input changes so that it affects the browser, while the node process gets the inputs of every user of a platform and can be killed that way. This problem has been patched in version 3.0.2. Users are	https://github.com/zxcvbn-ts/zxcvbn/commit/3f9bed21b5d01f6f6863476822ca857355fba22f, https://github.com/zxcvbn-ts/zxcvbn/security/advisories/GHSA-38hx-x5hq-5fg4	A-ZXC-ZXCV-280623/790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			advised to upgrade. Users unable to upgrade should stop using the second argument of the zxcvbn function and use the zxcvbnOptions.setOptions function. **CVE ID : CVE-2023-34109**		
Hardware					
Vendor: ABB					
Product: aspect-ent-12					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd.	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-ASPE-260623/791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-ASPE-260623/792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: aspect-ent-2					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-ASPE-260623/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&	H-ABB-ASPE-260623/794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**	Action=Launch	
Product: aspect-ent-256					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01.	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-ASPE-260623/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0635		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-ASPE-260623/796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: aspect-ent-96					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-ASPE-260623/797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-ASPE-260623/798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: matrix-11					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-MATR-260623/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-MATR-260623/800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: matrix-216					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on	https://search.abb.com/library/Download.aspx?DocumentID=2CKA0	H-ABB-MATR-260623/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**	00073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1.	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-MATR-260623/802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0636		
Product: matrix-232					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-MATR-260623/803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-MATR-260623/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: matrix-264					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-MATR-260623/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-MATR-260623/806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: matrix-296					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&	H-ABB-MATR-260623/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**	Action=Launch	
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on	https://search.abb.com/library/Download.aspx?DocumentID=2CKA0	H-ABB-MATR-260623/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**	00073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nexus-2128					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-NEXU-260623/809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-NEXU-260623/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: nexus-2128-a					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-NEXU-260623/811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-NEXU-260623/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: nexus-2128-f					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-NEXU-260623/813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&	H-ABB-NEXU-260623/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**	Action=Launch	
Product: nexus-2128-g					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management	https://search.abb.com/lib	H-ABB-NEXU-260623/815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01.	rary/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0635		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-NEXU-260623/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: nexus-264					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-NEXU-260623/817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd.	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-NEXU-260623/818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: nexus-264-a					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-NEXU-260623/819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-NEXU-260623/820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: nexus-264-f					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403	H-ABB-NEXU-260623/821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**	&LanguageCode=en&DocumentPartId=&Action=Launch	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1.	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-NEXU-260623/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0636		
Product: nexus-264-g					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-NEXU-260623/823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-NEXU-260623/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: nexus-3-2128					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-NEXU-260623/825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-NEXU-260623/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: nexus-3-264					
Affected Version(s): -					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&	H-ABB-NEXU-260623/827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**	Action=Launch	
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on	https://search.abb.com/library/Download.aspx?DocumentID=2CKA0	H-ABB-NEXU-260623/828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**	00073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Asus					
Product: rt-ac86u					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Jun-2023	8.8	ASUS RT-AC86U does not filter special characters for parameters in specific web URLs. A remote attacker with normal user privileges can exploit this vulnerability to perform command injection attack to execute arbitrary system commands, disrupt system or terminate service. **CVE ID : CVE-2023-28702**	N/A	H-ASU-RT-A-260623/829
Out-of-bounds Write	02-Jun-2023	7.2	ASUS RT-AC86U's specific cgi function has a stack-based buffer overflow vulnerability due to insufficient validation for network packet header length. A remote attacker with administrator privileges can exploit this vulnerability to execute arbitrary system commands, disrupt system or terminate service. **CVE ID : CVE-2023-28703**	N/A	H-ASU-RT-A-260623/830
Vendor: besder					
Product: bes--6024pb-i50h1					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Jun-2023	9.8	Incorrect access control in the administrative functionalities of BES--6024PB-I50H1 VideoPlayTool v2.0.1.0 allow attackers to execute arbitrary administrative commands via a crafted payload sent to the desired endpoints. **CVE ID : CVE-2023-33443**	N/A	H-BES-BES--260623/831
Vendor: danfoss					
Product: ak-em100					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Jun-2023	9.8	The Danfoss AK-EM100 web forms allow for SQL injection in the login forms. **CVE ID : CVE-2023-22583**	N/A	H-DAN-AK-E-260623/832
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Jun-2023	9.8	The Danfoss AK-EM100 web applications allow for OS command injection through the web application parameters. **CVE ID : CVE-2023-25911**	N/A	H-DAN-AK-E-260623/833
Cleartext Storage of Sensitive	11-Jun-2023	7.5	The Danfoss AK-EM100 stores login	N/A	H-DAN-AK-E-260623/834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			credentials in cleartext. **CVE ID : CVE-2023-22584**		
Exposure of Sensitive Information to an Unauthorized Actor	11-Jun-2023	7.5	The Danfoss AK-EM100 web applications allow for Local File Inclusion in the file parameter. **CVE ID : CVE-2023-22586**	N/A	H-DAN-AK-E-260623/835
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jun-2023	6.1	The Danfoss AK-EM100 web applications allow for Reflected Cross-Site Scripting. **CVE ID : CVE-2023-22582**	N/A	H-DAN-AK-E-260623/836
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jun-2023	6.1	The Danfoss AK-EM100 web applications allow for Reflected Cross-Site Scripting in the title parameter. **CVE ID : CVE-2023-22585**	N/A	H-DAN-AK-E-260623/837
Exposure of Sensitive Information to an Unauthorized Actor	11-Jun-2023	5.3	The webreport generation feature in the Danfoss AK-EM100 allows an unauthorized actor to generate a web report that discloses sensitive information such as the internal IP address, usernames and internal device values.	N/A	H-DAN-AK-E-260623/838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25912		
Vendor: Dlink					
Product: di-7500g-ci					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	5.4	A Cross Site Scripting (XSS) vulnerability in D-Link DI-7500G-CI-19.05.29A allows attackers to execute arbitrary code via uploading a crafted HTML file to the interface /auth_pic.cgi. **CVE ID : CVE-2023-34856**	N/A	H-DLI-DI-7-260623/839
Product: dir-842v2					
Affected Version(s): -					
N/A	07-Jun-2023	8.8	An issue in D-Link DIR-842V2 v1.0.3 allows attackers to execute arbitrary commands via importing a crafted file. **CVE ID : CVE-2023-33781**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--260623/840
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jun-2023	8.8	D-Link DIR-842V2 v1.0.3 was discovered to contain a command injection vulnerability via the iperf3 diagnostics function. **CVE ID : CVE-2023-33782**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--260623/841
Vendor: Draytek					
Product: vigor1000b					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/842
Product: vigor130					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected	N/A	H-DRA-VIGO-260623/843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor165					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/844
Product: vigor166					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points	N/A	H-DRA-VIGO-260623/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor167					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and	N/A	H-DRA-VIGO-260623/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2135ac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/847
Product: vigor2135ax					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware	N/A	H-DRA-VIGO-260623/848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2135fvac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/849
Product: vigor2135vac					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/850
Product: vigor2620l					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected	N/A	H-DRA-VIGO-260623/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2620ln					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/852
Product: vigor2763ac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points	N/A	H-DRA-VIGO-260623/853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2765ac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and	N/A	H-DRA-VIGO-260623/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2765ax					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/855
Product: vigor2765vac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware	N/A	H-DRA-VIGO-260623/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2766ac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/857
Product: vigor2766ax					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/858
Product: vigor2766vac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected	N/A	H-DRA-VIGO-260623/859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2832n					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/860
Product: vigor2862ac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points	N/A	H-DRA-VIGO-260623/861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2862b					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and	N/A	H-DRA-VIGO-260623/862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2862bn					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/863
Product: vigor2862l					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware	N/A	H-DRA-VIGO-260623/864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2862lac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/865
Product: vigor2862ln					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/866
Product: vigor2862n					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected	N/A	H-DRA-VIGO-260623/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2862vac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/868
Product: vigor2865ac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points	N/A	H-DRA-VIGO-260623/869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2865ax					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and	N/A	H-DRA-VIGO-260623/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2865l					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/871
Product: vigor2865lac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware	N/A	H-DRA-VIGO-260623/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2865vac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/873
Product: vigor2866ac					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/874
Product: vigor2866ax					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected	N/A	H-DRA-VIGO-260623/875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2866l					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/876
Product: vigor2866lac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points	N/A	H-DRA-VIGO-260623/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2866vac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and	N/A	H-DRA-VIGO-260623/878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2915ac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/879
Product: vigor2926_plus					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware	N/A	H-DRA-VIGO-260623/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2927ac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/881
Product: vigor2927ax					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/882
Product: vigor2927f					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected	N/A	H-DRA-VIGO-260623/883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2927l					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/884
Product: vigor2927lac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points	N/A	H-DRA-VIGO-260623/885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2927vac					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and	N/A	H-DRA-VIGO-260623/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2962					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/887
Product: vigor3910					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware	N/A	H-DRA-VIGO-260623/888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorap_1000c					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/889
Product: vigorap_1060c					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/890
Product: vigorap_903					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected	N/A	H-DRA-VIGO-260623/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorap_906					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/892
Product: vigorap_912c					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points	N/A	H-DRA-VIGO-260623/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorap_918r					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and	N/A	H-DRA-VIGO-260623/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorap_960c					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/895
Product: vigorlte_200n					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware	N/A	H-DRA-VIGO-260623/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorswitch_fx2120					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/897
Product: vigorswitch_g1080					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/898
Product: vigorswitch_g1085					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected	N/A	H-DRA-VIGO-260623/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorswitch_g1282					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/900
Product: vigorswitch_g2100					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points	N/A	H-DRA-VIGO-260623/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorswitch_g2121					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and	N/A	H-DRA-VIGO-260623/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorswitch_g2280x					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/903
Product: vigorswitch_g2540xs					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware	N/A	H-DRA-VIGO-260623/904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorswitch_p1282					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/905
Product: vigorswitch_p2100					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/906
Product: vigorswitch_p2280x					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected	N/A	H-DRA-VIGO-260623/907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorswitch_p2540xs					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/908
Product: vigorswitch_pq2121x					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points	N/A	H-DRA-VIGO-260623/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorswitch_pq2200xb					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and	N/A	H-DRA-VIGO-260623/910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorswitch_q2121x					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	H-DRA-VIGO-260623/911
Product: vigorswitch_q2200x					
Affected Version(s): -					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware	N/A	H-DRA-VIGO-260623/912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Vendor: fanuc					
Product: roboguide_handlingpro					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Jun-2023	7.5	FANUC ROBOGUIDE-HandlingPRO Versions 9 Rev.ZD and prior is vulnerable to a path traversal, which could allow an attacker to remotely read files on the system running the affected software. **CVE ID : CVE-2023-1864**	N/A	H-FAN-ROBO-260623/913
Vendor: furbo					
Product: dog_camera					
Affected Version(s): -					
Improper Neutralization of Special	02-Jun-2023	8.8	Furbo dog camera has insufficient filtering for special parameter of device log	N/A	H-FUR-DOG_-260623/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			management function. An unauthenticated remote attacker in the Bluetooth network with normal user privileges can exploit this vulnerability to perform command injection attack to execute arbitrary system commands or disrupt service. **CVE ID : CVE-2023-28704**		
Vendor: gallagher					
Product: controller_6000					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jun-2023	9.8	Controller 6000 is vulnerable to a buffer overflow via the Controller diagnostic web interface upload feature. This issue affects Controller 6000: before vCR8.80.230201a, before vCR8.70.230201a, before vCR8.60.230201b, before vCR8.50.230201a, all versions of vCR8.40 and prior.	https://security.gallagher.com/en-NZ/Security-Advisories/CVE-2023-24584	H-GAL-CONT-260623/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24584		
Vendor: harmonicinc					
Product: nsg_9000-6g					
Affected Version(s): -					
Missing Authorization	06-Jun-2023	6.5	In Harmonic NSG 9000-6G devices, an authenticated remote user can obtain source code by directly requesting a special path. **CVE ID : CVE-2023-33477**	N/A	H-HAR-NSG_-260623/916
Vendor: hitrontech					
Product: coda-5310					
Affected Version(s): -					
Improper Authentication	02-Jun-2023	9.8	Hitron Technologies CODA-5310 Telnet function with the default account and password, and there is no warning or prompt to ask users to change the default password and account. An unauthenticated remote attackers can exploit this vulnerability to obtain the administrator's privilege, resulting in performing arbitrary system operation or disrupt service. **CVE ID : CVE-2023-30603**	N/A	H-HIT-CODA-260623/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	02-Jun-2023	9.8	It is identified a vulnerability of insufficient authentication in the system configuration interface of Hitron Technologies CODA-5310. An unauthorized remote attacker can exploit this vulnerability to access system configuration interface, resulting in performing arbitrary system operation or disrupt service. **CVE ID : CVE-2023-30604**	N/A	H-HIT-CODA-260623/918
Missing Encryption of Sensitive Data	02-Jun-2023	7.5	Hitron Technologies CODA-5310's Telnet function transfers sensitive data in plaintext. An unauthenticated remote attacker can exploit this vulnerability to access credentials of normal users and administrator. **CVE ID : CVE-2023-30602**	N/A	H-HIT-CODA-260623/919
Vendor: mediatek					
Product: mt5221					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege	https://corp.mediatek.com/product-security-	H-MED-MT52-260623/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	bulletin/June-2023	
Product: mt5521					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT55-260623/921
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT55-260623/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt5696					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT56-260623/923
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT56-260623/924
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due 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/June-2023	H-MED-MT56-260623/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT56-260623/926
Product: mt5836					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT58-260623/927
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT58-260623/928

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: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT58-260623/929
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT58-260623/930
Product: mt5838					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT58-260623/931
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT58-260623/932
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT58-260623/933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT58-260623/934
Product: mt6580					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only).	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT65-260623/935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20725		
Product: mt6735					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/936
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/937
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**		
Product: mt6737					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/939
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/941
Product: mt6739					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/943
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/944
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**		
Product: mt6753					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/946
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/947
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT67-260623/948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	bulletin/June-2023	
Product: mt6757					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/949
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20741		
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/951
Product: mt6757c					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/952
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**		
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/954
Product: mt6757cd					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/956
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/957
Product: mt6757ch					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**		
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/959
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/960
Product: mt6761					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT67-260623/961

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: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/962
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/964
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/965
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**		
Product: mt6762					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/967
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/969
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/970
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**		
Product: mt6763					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/972
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/973
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT67-260623/974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	bulletin/June-2023	
Product: mt6765					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/975
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/977
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/978
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT67-260623/979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/980
Product: mt6768					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890,	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/982
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/983
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing	https://corp.mediatek.com/product-	H-MED-MT67-260623/984

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: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	security-bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/985
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/987
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/988
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/990
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/991
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**		
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/993
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/994
Product: mt6769					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/995
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/996
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/998
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/999
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a 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/June-2023	H-MED-MT67-260623/1000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1001
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1002
Concurrent Execution using Shared Resource	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT67-260623/1003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1004
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1006
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1007
Product: mt6771					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**		
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1009
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1010
Product: mt6779					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT67-260623/1011

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: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1012
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1014
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1015
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1017
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1018
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a	https://corp.mediatek.com/product-	H-MED-MT67-260623/1019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	security-bulletin/June-2023	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1020
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1022
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1023
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**		
Product: mt6781					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1025
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20732		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1027
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1028
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due 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/June-2023	H-MED-MT67-260623/1029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1030
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1031
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1033
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1034
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT67-260623/1035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1036
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1038
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1039
Product: mt6785					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due 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/June-2023	H-MED-MT67-260623/1040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1041
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20733		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1043
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1044
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1046
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1047
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1049
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1050
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT67-260623/1051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1052
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1053
Product: mt6789					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1054
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1055
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**		
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1057
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1059
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1060
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1062
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1063
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1065
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519142. **CVE ID : CVE-2023-20743**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1066
Use After Free	06-Jun-2023	6.7	In vcu, there is a possible use after free due to a logic error. This could lead to local escalation of	https://corp.mediatek.com/product-security-	H-MED-MT67-260623/1067

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: ALPS07519142; Issue ID: ALPS07519200. **CVE ID : CVE-2023-20744**	bulletin/June-2023	
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07560694. **CVE ID : CVE-2023-20745**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1068
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1070
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1071
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1073
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1074
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**		
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1076
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT67-260623/1077
Product: mt6833					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1078
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1079
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT68-260623/1080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1081
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1082
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free	https://corp.mediatek.com	H-MED-MT68-260623/1083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	/product-security-bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1084
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20739		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1086
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1087
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1089
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1090
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1092
Product: mt6835					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 /	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1094
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1095
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**		
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1097
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1098
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing	https://corp.mediatek.com/product-	H-MED-MT68-260623/1099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	security-bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1100
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1102
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1103
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**		
Product: mt6853					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1105
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20732		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1107
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1108
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due 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/June-2023	H-MED-MT68-260623/1109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1110
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1111
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1113
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1114
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT68-260623/1115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1116
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1118
Product: mt6853t					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1119
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free	https://corp.mediatek.com	H-MED-MT68-260623/1120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	/product-security-bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1121
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20735		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1123
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1124
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1126
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1127
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**		
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1129
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1130
Product: mt6855					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1131
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1132
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**		
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1134
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1136
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1137
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07519142; Issue ID: ALPS07519142. **CVE ID : CVE-2023-20743**		
Use After Free	06-Jun-2023	6.7	In vcu, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519200. **CVE ID : CVE-2023-20744**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1139
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07560694. **CVE ID : CVE-2023-20745**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1140
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**		
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1142
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1143
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT68-260623/1144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1145
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1147
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1148
Product: mt6873					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due 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/June-2023	H-MED-MT68-260623/1149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1150
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20733		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1152
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1153
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1155
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1156
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1158
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1159
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT68-260623/1160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1161
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1162
Product: mt6875					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1163
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1164
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1166
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1167
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a 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/June-2023	H-MED-MT68-260623/1168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1169
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1170
Concurrent Execution using Shared Resource	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT68-260623/1171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1172
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1174
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1175
Product: mt6877					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due 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/June-2023	H-MED-MT68-260623/1176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1177
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20733		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1179
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1180
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1182
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1183
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1185
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1186
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT68-260623/1187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1188
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1190
Product: mt6879					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1191
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1193
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only).	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20725		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1195
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1196
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due 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/June-2023	H-MED-MT68-260623/1197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1198
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1199
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**		
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1201
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1202
Product: mt6880					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1203
Product: mt6883					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1205
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1206
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1208
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1209
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT68-260623/1210

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: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1211
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1213
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1214
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**		
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1216
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1217
Product: mt6885					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, 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-	H-MED-MT68-260623/1218

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: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1219
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1221
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1222
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1224
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1225
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-260623/1226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	bulletin/June-2023	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1227
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1229
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1230
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**		
Product: mt6886					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1232
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20732		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1234
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1235
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1237
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1238
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**		
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1240
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1241
Product: mt6889					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1242
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1243
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT68-260623/1244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1245
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1246
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free	https://corp.mediatek.com	H-MED-MT68-260623/1247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	/product-security-bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1248
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20739		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1250
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1251
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**		
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1253
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1254
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**		
Product: mt6890					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1256
Product: mt6891					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1258
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1259
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing	https://corp.mediatek.com/product-	H-MED-MT68-260623/1260

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: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	security-bulletin/June-2023	
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1261
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1263
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1264
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1266
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1267
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1269
Product: mt6893					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1271
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1272
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1274
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1275
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT68-260623/1276

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: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1277
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1279
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1280
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**		
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1282
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1283
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**		
Product: mt6895					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1285
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1287
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1288
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT68-260623/1289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1290
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1292
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1293
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**		
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1295
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT68-260623/1296
Product: mt6980					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, 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-	H-MED-MT69-260623/1297

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: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	bulletin/June-2023	
Product: mt6983					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1298
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1300
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890,	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MT6980, MT6990 only). **CVE ID : CVE-2023-20725**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1302
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1303
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a 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/June-2023	H-MED-MT69-260623/1304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1305
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1306
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT69-260623/1307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1308
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1309
Concurrent Execution	06-Jun-2023	4.1	In swpm, there is a possible out of bounds	https://corp.mediatek.com	H-MED-MT69-260623/1310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	/product-security-bulletin/June-2023	
Product: mt6985					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1311
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT69-260623/1312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1313
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1315
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1316
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07573552; Issue ID: ALPS07573575. **CVE ID : CVE-2023-20729**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573552. **CVE ID : CVE-2023-20730**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1318
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1319
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**		
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1321
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1322
Product: mt6990					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT69-260623/1323
Product: mt7663					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT76-260623/1324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT76-260623/1325
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT76-260623/1326
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT76-260623/1327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT76-260623/1328
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT76-260623/1329
Product: mt7668					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, 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-	H-MED-MT76-260623/1330

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: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT76-260623/1331
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT76-260623/1332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT76-260623/1333
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT76-260623/1334
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT76-260623/1335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**		
Product: mt7902					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT79-260623/1336
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT79-260623/1337
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, 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-	H-MED-MT79-260623/1338

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: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT79-260623/1339
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT79-260623/1340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573575. **CVE ID : CVE-2023-20729**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT79-260623/1341
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573552. **CVE ID : CVE-2023-20730**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT79-260623/1342
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT79-260623/1343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**		
Product: mt7921					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT79-260623/1344
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT79-260623/1345
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, 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-	H-MED-MT79-260623/1346

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: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT79-260623/1347
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT79-260623/1348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573575. **CVE ID : CVE-2023-20729**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT79-260623/1349
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573552. **CVE ID : CVE-2023-20730**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT79-260623/1350
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT79-260623/1351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**		
Product: mt8167					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	6.7	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07843845; Issue ID: ALPS07843845. **CVE ID : CVE-2023-20723**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1352
Out-of-bounds Read	06-Jun-2023	6.7	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07843845; Issue ID: ALPS07843841. **CVE ID : CVE-2023-20724**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1353
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, 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-	H-MED-MT81-260623/1354

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: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1355
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1357
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1358
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07825502; Issue ID: ALPS07825502. **CVE ID : CVE-2023-20751**		
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826586; Issue ID: ALPS07826586. **CVE ID : CVE-2023-20752**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1360
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1361
Concurrent Execution	06-Jun-2023	4.1	In swpm, there is a possible out of bounds	https://corp.mediatek.com	H-MED-MT81-260623/1362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	/product-security-bulletin/June-2023	
Product: mt8167s					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1363
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1365
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1366
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a 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/June-2023	H-MED-MT81-260623/1367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**		
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07825502; Issue ID: ALPS07825502. **CVE ID : CVE-2023-20751**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1368
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826586; Issue ID: ALPS07826586. **CVE ID : CVE-2023-20752**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1369
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing	https://corp.mediatek.com/product-	H-MED-MT81-260623/1370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	security-bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1371
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt8168					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1373
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1374
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1376
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1377
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1379
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1380
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could	https://corp.mediatek.com/product-security-	H-MED-MT81-260623/1381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	bulletin/June-2023	
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1382
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07825502; Issue ID: ALPS07825502. **CVE ID : CVE-2023-20751**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1384
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826586; Issue ID: ALPS07826586. **CVE ID : CVE-2023-20752**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1385
Concurrent Execution using Shared Resource with Improper Synchronization	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1387
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1388
Concurrent Execution using Shared Resource with Improper Synchroniz	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**		
Product: mt8173					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1390
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1391
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds	https://corp.mediatek.com	H-MED-MT81-260623/1392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	/product-security-bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1393
Product: mt8175					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1395
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1396
Out-of-bounds Read	06-Jun-2023	6.7	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07843845; Issue ID: ALPS07843845. **CVE ID : CVE-2023-20723**		
Out-of-bounds Read	06-Jun-2023	6.7	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07843845; Issue ID: ALPS07843841. **CVE ID : CVE-2023-20724**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1398
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890,	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MT6980, MT6990 only). **CVE ID : CVE-2023-20725**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1400
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1401
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a 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/June-2023	H-MED-MT81-260623/1402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**		
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1403
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07825502; Issue ID: ALPS07825502. **CVE ID : CVE-2023-20751**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1404
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check.	https://corp.mediatek.com/product-security-	H-MED-MT81-260623/1405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826586; Issue ID: ALPS07826586. **CVE ID : CVE-2023-20752**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1406
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1408
Product: mt8183					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	6.7	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07843845; Issue ID: ALPS07843845. **CVE ID : CVE-2023-20723**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1409
Out-of-bounds Read	06-Jun-2023	6.7	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07843845; Issue ID: ALPS07843841. **CVE ID : CVE-2023-20724**		
Product: mt8185					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1411
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519142. **CVE ID : CVE-2023-20743**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1412
Use After Free	06-Jun-2023	6.7	In vcu, there is a possible use after free due to a logic error. This could lead to	https://corp.mediatek.com/product-security-	H-MED-MT81-260623/1413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519200. **CVE ID : CVE-2023-20744**	bulletin/June-2023	
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07560694. **CVE ID : CVE-2023-20745**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1414
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1416
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1417
Product: mt8195					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due 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/June-2023	H-MED-MT81-260623/1418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1419
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20735		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1421
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519142. **CVE ID : CVE-2023-20743**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1422
Use After Free	06-Jun-2023	6.7	In vcu, there is a possible use after free due to a logic error. 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/June-2023	H-MED-MT81-260623/1423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519200. **CVE ID : CVE-2023-20744**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07560694. **CVE ID : CVE-2023-20745**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1424
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1425
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**		
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07825502; Issue ID: ALPS07825502. **CVE ID : CVE-2023-20751**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1427
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826586; Issue ID: ALPS07826586. **CVE ID : CVE-2023-20752**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1429
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1430
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT81-260623/1432
Product: mt8321					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1433
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT83-260623/1434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	bulletin/June-2023	
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1435
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1437
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1438
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**		
Product: mt8362a					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1440
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1441
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, 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-	H-MED-MT83-260623/1442

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: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1443
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07825502; Issue ID: ALPS07825502. **CVE ID : CVE-2023-20751**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1445
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826586; Issue ID: ALPS07826586. **CVE ID : CVE-2023-20752**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1446
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1448
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1449
Product: mt8365					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, 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-	H-MED-MT83-260623/1450

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: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1451
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1453
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1454
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT83-260623/1455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1456
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1457
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free	https://corp.mediatek.com	H-MED-MT83-260623/1458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	/product-security-bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1459
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20740		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519142. **CVE ID : CVE-2023-20743**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1461
Use After Free	06-Jun-2023	6.7	In vcu, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519200. **CVE ID : CVE-2023-20744**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1462
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. 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/June-2023	H-MED-MT83-260623/1463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07560694. **CVE ID : CVE-2023-20745**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1464
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1465
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07825502; Issue ID: ALPS07825502. **CVE ID : CVE-2023-20751**		
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826586; Issue ID: ALPS07826586. **CVE ID : CVE-2023-20752**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1467
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1469
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1470
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07573552; Issue ID: ALPS07573575. **CVE ID : CVE-2023-20729**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573552. **CVE ID : CVE-2023-20730**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1472
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1473
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1475
Product: mt8385					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1477
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1478
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1480
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1482
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1483
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**		
Product: mt8395					
Affected Version(s): -					
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1485
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1486
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, 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-	H-MED-MT83-260623/1487

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: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	bulletin/June-2023	
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1488
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1490
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519142. **CVE ID : CVE-2023-20743**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1491
Use After Free	06-Jun-2023	6.7	In vcu, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07519142; Issue ID: ALPS07519200. **CVE ID : CVE-2023-20744**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07560694. **CVE ID : CVE-2023-20745**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1493
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1494
Concurrent Execution using Shared Resource with Improper Synchroniz	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT83-260623/1496
Product: mt8518					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT85-260623/1497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT85-260623/1498
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT85-260623/1499
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT85-260623/1500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT85-260623/1501
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573575. **CVE ID : CVE-2023-20729**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT85-260623/1502
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT85-260623/1503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573552. **CVE ID : CVE-2023-20730**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT85-260623/1504
Product: mt8532					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT85-260623/1505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT85-260623/1506
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT85-260623/1507
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT85-260623/1508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT85-260623/1509
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573575. **CVE ID : CVE-2023-20729**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT85-260623/1510
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT85-260623/1511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573552. **CVE ID : CVE-2023-20730**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT85-260623/1512
Product: mt8666					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT86-260623/1513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT86-260623/1514
Product: mt8673					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT86-260623/1515
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT86-260623/1516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT86-260623/1517
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only).	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT86-260623/1518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20725		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT86-260623/1519
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT86-260623/1520
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due 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/June-2023	H-MED-MT86-260623/1521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT86-260623/1522
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT86-260623/1523
Product: mt8675					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT86-260623/1524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	bulletin/June-2023	
Product: mt8695					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT86-260623/1525
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT86-260623/1526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20716		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT86-260623/1527
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT86-260623/1528
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT86-260623/1529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT86-260623/1530
Product: mt8765					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1531
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could	https://corp.mediatek.com/product-security-	H-MED-MT87-260623/1532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	bulletin/June-2023	
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1533
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1535
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1536
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**		
Product: mt8766					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1538
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1539
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, 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-	H-MED-MT87-260623/1540

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: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1541
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1542
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds	https://corp.mediatek.com	H-MED-MT87-260623/1543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	/product-security-bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1544
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20727		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1546
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1547
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1549
Product: mt8768					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1550
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT87-260623/1551

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: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1552
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1554
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1555
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1557
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1558
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**		
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1560
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1561
Product: mt8781					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1562
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1563
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**		
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1565
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1567
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1568
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1570
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519142. **CVE ID : CVE-2023-20743**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1571
Use After Free	06-Jun-2023	6.7	In vcu, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519200. **CVE ID : CVE-2023-20744**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07560694. **CVE ID : CVE-2023-20745**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1573
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1574
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, 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-	H-MED-MT87-260623/1575

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: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1576
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1578
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1579
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1581
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1582
Product: mt8786					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, 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-	H-MED-MT87-260623/1583

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: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1584
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1586
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1587
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1589
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519142. **CVE ID : CVE-2023-20743**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1590
Use After Free	06-Jun-2023	6.7	In vcu, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519200. **CVE ID : CVE-2023-20744**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07560694. **CVE ID : CVE-2023-20745**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1592
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1593
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, 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-	H-MED-MT87-260623/1594

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: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1595
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1597
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1598
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1600
Product: mt8788					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1601
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, 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-	H-MED-MT87-260623/1602

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: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1603
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1605
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1606
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1608
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1609
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT87-260623/1610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1611
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1613
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1614
Product: mt8789					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1616
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1617
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1619
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1621
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1622
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519142. **CVE ID : CVE-2023-20743**		
Use After Free	06-Jun-2023	6.7	In vcu, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519200. **CVE ID : CVE-2023-20744**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1624
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07560694. **CVE ID : CVE-2023-20745**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1625
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT87-260623/1626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1627
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1629
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1630
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**		
Product: mt8791					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1632
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1633
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, 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-	H-MED-MT87-260623/1634

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: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1635
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519142. **CVE ID : CVE-2023-20743**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1636
Use After Free	06-Jun-2023	6.7	In vcu, there is a possible use after free	https://corp.mediatek.com	H-MED-MT87-260623/1637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519200. **CVE ID : CVE-2023-20744**	/product-security-bulletin/June-2023	
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07560694. **CVE ID : CVE-2023-20745**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1638
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217.	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20746		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1640
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1641
Product: mt8791t					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a 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/June-2023	H-MED-MT87-260623/1642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1643
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1644
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation	https://corp.mediatek.com/product-security-	H-MED-MT87-260623/1645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	bulletin/June-2023	
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1646
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1648
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1649
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**		
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1651
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1652
Product: mt8797					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, 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-	H-MED-MT87-260623/1653

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: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1654
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1656
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1657
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1659
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519142. **CVE ID : CVE-2023-20743**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1660
Use After Free	06-Jun-2023	6.7	In vcu, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519200. **CVE ID : CVE-2023-20744**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07560694. **CVE ID : CVE-2023-20745**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1662
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1663
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, 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-	H-MED-MT87-260623/1664

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: ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1665
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1667
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1668
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT87-260623/1670
Product: mt9000					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT90-260623/1671
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, 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-	H-MED-MT90-260623/1672

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: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT90-260623/1673
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT90-260623/1674
Product: mt9015					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT90-260623/1675
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT90-260623/1676
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT90-260623/1677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT90-260623/1678
Product: mt9023					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT90-260623/1679
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, 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-	H-MED-MT90-260623/1680

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: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT90-260623/1681
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT90-260623/1682
Product: mt9025					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT90-260623/1683
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT90-260623/1684
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT90-260623/1685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT90-260623/1686
Product: mt9618					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1687
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, 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-	H-MED-MT96-260623/1688

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: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1689
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1690
Product: mt9649					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1691
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1692
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1694
Product: mt9653					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1695
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, 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-	H-MED-MT96-260623/1696

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: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1697
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1698
Product: mt9679					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1699
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1700
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1702
Product: mt9687					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1703
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, 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-	H-MED-MT96-260623/1704

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: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1705
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1706
Product: mt9689					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1707
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1708
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT96-260623/1710
Product: mt9902					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT99-260623/1711
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, 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-	H-MED-MT99-260623/1712

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: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT99-260623/1713
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT99-260623/1714
Product: mt9932					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT99-260623/1715
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT99-260623/1716
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT99-260623/1717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT99-260623/1718
Product: mt9952					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT99-260623/1719
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, 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-	H-MED-MT99-260623/1720

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: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT99-260623/1721
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT99-260623/1722
Product: mt9972					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT99-260623/1723
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT99-260623/1724
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT99-260623/1725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT99-260623/1726
Product: mt9982					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT99-260623/1727
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, 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-	H-MED-MT99-260623/1728

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: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT99-260623/1729
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	H-MED-MT99-260623/1730
Vendor: mitrastar					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: gpt-2741gnac					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jun-2023	7.2	A command injection vulnerability was found in the ping functionality of the MitraStar GPT-2741GNAC router (firmware version AR_g5.8_110WVN0b7_2). The vulnerability allows an authenticated user to execute arbitrary OS commands by sending specially crafted input to the router via the ping function. **CVE ID : CVE-2023-33381**	N/A	H-MIT-GPT--260623/1731
Vendor: Netgear					
Product: d6220					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jun-2023	8.8	Netgear D6220 with Firmware Version 1.0.0.80, D8500 with Firmware Version 1.0.3.60, R6700 with Firmware Version 1.0.2.26, and R6900 with Firmware Version 1.0.2.26 are vulnerable to Command Injection. If an attacker gains web management privileges, they can inject commands into the post request parameters, gaining shell privileges.	https://www.netgear.com/about/security/	H-NET-D622-260623/1732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33533		
Product: d8500					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jun-2023	8.8	Netgear D6220 with Firmware Version 1.0.0.80, D8500 with Firmware Version 1.0.3.60, R6700 with Firmware Version 1.0.2.26, and R6900 with Firmware Version 1.0.2.26 are vulnerable to Command Injection. If an attacker gains web management privileges, they can inject commands into the post request parameters, gaining shell privileges. **CVE ID : CVE-2023-33533**	https://www.netgear.com/about/security/	H-NET-D850-260623/1733
Product: r6250					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jun-2023	9.8	There is a command injection vulnerability in the Netgear R6250 router with Firmware Version 1.0.4.48. If an attacker gains web management privileges, they can inject commands into the post request parameters, thereby gaining shell privileges. **CVE ID : CVE-2023-33532**	N/A	H-NET-R625-260623/1734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: r6700					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jun-2023	8.8	Netgear D6220 with Firmware Version 1.0.0.80, D8500 with Firmware Version 1.0.3.60, R6700 with Firmware Version 1.0.2.26, and R6900 with Firmware Version 1.0.2.26 are vulnerable to Command Injection. If an attacker gains web management privileges, they can inject commands into the post request parameters, gaining shell privileges. **CVE ID : CVE-2023-33533**	https://www.netgear.com/about/security/	H-NET-R670-260623/1735
Product: r6900					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jun-2023	8.8	Netgear D6220 with Firmware Version 1.0.0.80, D8500 with Firmware Version 1.0.3.60, R6700 with Firmware Version 1.0.2.26, and R6900 with Firmware Version 1.0.2.26 are vulnerable to Command Injection. If an attacker gains web management privileges, they can inject commands into the post request parameters, gaining shell privileges.	https://www.netgear.com/about/security/	H-NET-R690-260623/1736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33533		
Vendor: planet					
Product: wdrt-1800ax					
Affected Version(s): -					
Improper Authentication	07-Jun-2023	9.8	An issue in Planet Technologies WDRT-1800AX v1.01-CP21 allows attackers to bypass authentication and escalate privileges to root via manipulation of the LoginStatus cookie. **CVE ID : CVE-2023-33553**	N/A	H-PLA-WDRT-260623/1737
Vendor: Qualcomm					
Product: 205_mobile_platform					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-205_-260623/1738
Product: 315_5g_iot_modem					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-315_-260623/1739
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	H-QUA-315_-260623/1740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Product: apq8017					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-APQ8-260623/1741
Product: apq8064au					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-APQ8-260623/1742
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-APQ8-260623/1743
Product: apq8076					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-APQ8-260623/1744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: apq8092					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-APQ8-260623/1745
Product: apq8094					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-APQ8-260623/1746
Product: aqt1000					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-AQT1-260623/1747
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-AQT1-260623/1748
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-AQT1-260623/1749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-AQT1-260623/1750
Product: ar8031					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-AR80-260623/1751
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-AR80-260623/1752
Product: ar8035					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-AR80-260623/1753
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-AR80-260623/1754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21656	tins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-AR80-260623/1755
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-AR80-260623/1756
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-AR80-260623/1757
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-AR80-260623/1758
Product: ar9380					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-AR93-260623/1759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-AR93-260623/1760
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-AR93-260623/1761
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-AR93-260623/1762
Product: c-v2x9150					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-C-V2-260623/1763
Product: csr8811					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-CSR8-260623/1764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-CSR8-260623/1765
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-CSR8-260623/1766
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-CSR8-260623/1767
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-CSR8-260623/1768
Product: csra6620					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-CSRA-260623/1769
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while	https://www.qualcomm.com/company/product-	H-QUA-CSRA-260623/1770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	security/bulletins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-CSRA-260623/1771
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-CSRA-260623/1772
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-CSRA-260623/1773
Product: csra6640					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-CSRA-260623/1774
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulle	H-QUA-CSRA-260623/1775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-CSRA-260623/1776
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-CSRA-260623/1777
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-CSRA-260623/1778
Product: csrb31024					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-CSRB-260623/1779
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-CSRB-260623/1780
Product: flight_rb5_5g_platform					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-FLIG-260623/1781
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-FLIG-260623/1782
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-FLIG-260623/1783
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-FLIG-260623/1784
Product: home_hub_100_platform					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-HOME-260623/1785
Product: immersive_home_214_platform					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1786
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1787
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1788
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1789
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1790
Product: immersive_home_216_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1791
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1792
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1793
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1794
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1795
Product: immersive_home_316_platform					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF	https://www.qualcomm.com/company/product-	H-QUA-IMME-260623/1796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1797
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1798
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1799
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1800
Product: immersive_home_318_platform					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-IMME-260623/1801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1802
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1803
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1804
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IMME-260623/1805
Product: ipq4018					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ4-260623/1806
Product: ipq4019					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ4-260623/1807
Product: ipq4028					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ4-260623/1808
Product: ipq4029					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ4-260623/1809
Product: ipq5010					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ5-260623/1810
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/product-	H-QUA-IPQ5-260623/1811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ5-260623/1812
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ5-260623/1813
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ5-260623/1814
Product: ipq5028					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ5-260623/1815
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-IPQ5-260623/1816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21658	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ5-260623/1817
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ5-260623/1818
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ5-260623/1819
Product: ipq6000					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1820
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1822
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1823
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1824
Product: ipq6005					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1825
Product: ipq6010					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1827
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1828
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1829
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1830
Product: ipq6018					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1831
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/product-	H-QUA-IPQ6-260623/1832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1833
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1834
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1835
Product: ipq6028					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1836
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-IPQ6-260623/1837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21658	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1838
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1839
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ6-260623/1840
Product: ipq8064					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1841
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1843
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1844
Product: ipq8065					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1845
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1846
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1847
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon	https://www.qualcomm.com/company/	H-QUA-IPQ8-260623/1848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or probe-response frame. **CVE ID : CVE-2023-21661**	product-security/bulletins/june-2023-bulletin	
Product: ipq8068					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1849
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1850
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1851
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1852
Product: ipq8069					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-260623/1853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	security/bulletins/june-2023-bulletin	
Product: ipq8070					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1854
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1855
Product: ipq8070a					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1856
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1857
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/	H-QUA-IPQ8-260623/1858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	product-security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1859
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1860
Product: ipq8071					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1861
Product: ipq8071a					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1862
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-260623/1863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1864
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1865
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1866
Product: ipq8072					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1867
Product: ipq8072a					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-260623/1868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1869
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1870
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1871
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1872
Product: ipq8074					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-IPQ8-260623/1873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Product: ipq8074a					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1874
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1875
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1876
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1877
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1878
Product: ipq8076					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1879
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1880
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1881
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1882
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1883
Product: ipq8076a					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1884
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1885
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1886
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1887
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1888
Product: ipq8078					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-260623/1889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1890
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1891
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1892
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1893
Product: ipq8078a					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-IPQ8-260623/1894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1895
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1896
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1897
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1898
Product: ipq8173					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1900
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1901
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1902
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1903
Product: ipq8174					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1904
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-260623/1905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1906
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1907
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ8-260623/1908
Product: ipq9008					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ9-260623/1909
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-IPQ9-260623/1910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ9-260623/1911
Product: ipq9574					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ9-260623/1912
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ9-260623/1913
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ9-260623/1914
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-IPQ9-260623/1915
Product: mdm8215					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-MDM8-260623/1916
Product: mdm9215					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-MDM9-260623/1917
Product: mdm9250					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-MDM9-260623/1918
Product: mdm9310					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-MDM9-260623/1919
Product: mdm9615					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-MDM9-260623/1920
Product: mdm9628					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-MDM9-260623/1921
Product: mdm9640					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-MDM9-260623/1922
Product: mdm9645					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-MDM9-260623/1923
Product: mdm9650					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-MDM9-260623/1924
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-MDM9-260623/1925
Product: msm8996au					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-MSM8-260623/1926
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-MSM8-260623/1927
Product: pmp8074					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-PMP8-260623/1928
Product: qam8255p					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1929
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1930
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1931
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1932
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1933
Product: qam8295p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1934
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1935
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1936
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1937
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1938
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QAM8-260623/1939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Product: qam8650p					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1940
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1941
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1942
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1943
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1944
Product: qam8775p					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1945
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1946
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1947
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1948
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QAM8-260623/1949
Product: qca0000					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA0-260623/1950
Product: qca1023					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA1-260623/1951
Product: qca1062					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA1-260623/1952
Product: qca1064					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA1-260623/1953
Product: qca1990					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA1-260623/1954
Product: qca2062					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA2-260623/1955
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA2-260623/1956
Product: qca2064					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA2-260623/1957
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA2-260623/1958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca2065					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA2-260623/1959
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA2-260623/1960
Product: qca2066					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA2-260623/1961
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA2-260623/1962
Product: qca4010					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA4-260623/1963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Product: qca4024					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA4-260623/1964
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA4-260623/1965
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA4-260623/1966
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA4-260623/1967
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA4-260623/1968
Product: qca4531					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA4-260623/1969
Product: qca6174					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1970
Product: qca6174a					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1971
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1972
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670		
Product: qca6175a					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1974
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1975
Product: qca6310					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1976
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1977
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA6-260623/1978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1979
Product: qca6320					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1980
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1981
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1982
Product: qca6335					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA6-260623/1983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1984
Product: qca6390					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1985
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1986
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1987
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1989
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1990
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1991
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1992
Product: qca6391					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1994
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1995
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1996
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1997
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/1998
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA6-260623/1999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2000
Product: qca6420					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2001
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2002
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2003
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address.	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21669		
Product: qca6421					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2005
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2006
Product: qca6426					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2007
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2008
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA6-260623/2009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2010
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2011
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2012
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2013
Product: qca6428					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca6430					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2015
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2016
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2017
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2018
Product: qca6431					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659		
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2020
Product: qca6436					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2021
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2022
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2023
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2025
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2026
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2027
Product: qca6438					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2028
Product: qca6554a					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2030
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2031
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2032
Product: qca6564					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2033
Product: qca6564a					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2035
Product: qca6564au					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2036
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2037
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2038
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2039
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	H-QUA-QCA6-260623/2040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Product: qca6574					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2041
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2042
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2043
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2044
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA6-260623/2045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21658	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2046
Product: qca6574a					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2047
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2048
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2049
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2051
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2052
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2053
Product: qca6574au					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2054
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2055
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while	https://www.qualcomm.com/company/	H-QUA-QCA6-260623/2056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	product-security/bulletins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2057
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2058
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2059
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2060
Product: qca6584					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA6-260623/2061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Product: qca6584au					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2062
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2063
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2064
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2065
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2066
Product: qca6595					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2067
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2068
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2069
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2070
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2071
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA6-260623/2072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21658	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2073
Product: qca6595au					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2074
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2075
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2076
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2078
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2079
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2080
Product: qca6678aq					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2081
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2082
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/	H-QUA-QCA6-260623/2083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	product-security/bulletins/june-2023-bulletin	
Product: qca6696					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2084
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2085
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2086
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2087
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670		
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2089
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2090
Product: qca6698aq					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2091
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2092
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2094
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2095
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2096
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2097
Product: qca6797aq					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2098
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP	https://www.qualcomm.com/company/product-	H-QUA-QCA6-260623/2099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sends input during record use case. **CVE ID : CVE-2023-21657**	security/bulletins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2100
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2101
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA6-260623/2102
Product: qca7500					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA7-260623/2103
Product: qca8072					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/	H-QUA-QCA8-260623/2104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	product-security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2105
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2106
Product: qca8075					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2107
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2108
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA8-260623/2109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2110
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2111
Product: qca8081					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2112
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2113
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2115
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2116
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2117
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2118
Product: qca8082					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2119
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	H-QUA-QCA8-260623/2120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2121
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2122
Product: qca8084					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2123
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2124
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA8-260623/2125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2126
Product: qca8085					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2127
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2128
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2129
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2130
Product: qca8337					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2131
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2132
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2133
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2134
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2135
Product: qca8386					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2136
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2137
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2138
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA8-260623/2139
Product: qca9367					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2140
Product: qca9377					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2141
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2142
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2143
Product: qca9379					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2144
Product: qca9531					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca9558					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2146
Product: qca9561					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2147
Product: qca9880					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2148
Product: qca9882					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2149
Product: qca9886					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2150
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2151
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2152
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2153
Product: qca9887					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2154
Product: qca9888					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2155
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2156
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2157
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2158
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2159
Product: qca9889					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF	https://www.qualcomm.com/company/product-	H-QUA-QCA9-260623/2160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2161
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2162
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2163
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2164
Product: qca9898					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA9-260623/2165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Product: qca9980					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2166
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2167
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2168
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2169
Product: qca9982					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA9-260623/2170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Product: qca9984					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2171
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2172
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2173
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2174
Product: qca9985					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA9-260623/2175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2176
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2177
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2178
Product: qca9986					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2179
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2181
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2182
Product: qca9990					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2183
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2184
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2185
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon	https://www.qualcomm.com/company/	H-QUA-QCA9-260623/2186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or probe-response frame. **CVE ID : CVE-2023-21661**	product-security/bulletins/june-2023-bulletin	
Product: qca9992					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2187
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2188
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2189
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2190
Product: qca9994					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF	https://www.qualcomm.com/company/product-	H-QUA-QCA9-260623/2191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2192
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2193
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCA9-260623/2194
Product: qcc2073					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCC2-260623/2195
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCC2-260623/2196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21658	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCC2-260623/2197
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCC2-260623/2198
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCC2-260623/2199
Product: qcc2076					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCC2-260623/2200
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCC2-260623/2201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCC2-260623/2202
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCC2-260623/2203
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCC2-260623/2204
Product: qcm2290					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM2-260623/2205
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM2-260623/2206
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command	https://www.qualcomm.com/company/product-	H-QUA-QCM2-260623/2207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM2-260623/2208
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM2-260623/2209
Product: qcm4290					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM4-260623/2210
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM4-260623/2211
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCM4-260623/2212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM4-260623/2213
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM4-260623/2214
Product: qcm4325					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM4-260623/2215
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM4-260623/2216
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM4-260623/2217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM4-260623/2218
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM4-260623/2219
Product: qcm4490					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM4-260623/2220
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM4-260623/2221
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM4-260623/2222
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/	H-QUA-QCM4-260623/2223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	product-security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM4-260623/2224
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM4-260623/2225
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM4-260623/2226
Product: qcm6125					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM6-260623/2227
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCM6-260623/2228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Product: qcm6490					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM6-260623/2229
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM6-260623/2230
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM6-260623/2231
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM6-260623/2232
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM6-260623/2233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCM6-260623/2234
Product: qcn5021					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2235
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2236
Product: qcn5022					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2237
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2239
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2240
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2241
Product: qcn5024					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2242
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2243
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	H-QUA-QCN5-260623/2244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2245
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2246
Product: qcn5052					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2247
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2248
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCN5-260623/2249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2250
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2251
Product: qcn5054					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2252
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2253
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2255
Product: qcn5064					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2256
Product: qcn5121					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2257
Product: qcn5122					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2258
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCN5-260623/2259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21658	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2260
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2261
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2262
Product: qcn5124					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2263
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2265
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2266
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2267
Product: qcn5152					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2268
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2269
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	H-QUA-QCN5-260623/2270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2271
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2272
Product: qcn5154					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2273
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2274
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCN5-260623/2275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2276
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2277
Product: qcn5164					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2278
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2279
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2281
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2282
Product: qcn5550					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN5-260623/2283
Product: qcn6023					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2284
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2286
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2287
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2288
Product: qcn6024					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2289
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2290
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command	https://www.qualcomm.com/company/product-	H-QUA-QCN6-260623/2291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2292
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2293
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2294
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2295
Product: qcn6100					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCN6-260623/2296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21658	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2297
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2298
Product: qcn6102					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2299
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2300
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2301
Product: qcn6112					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2302
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2303
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2304
Product: qcn6122					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2305
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2307
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2308
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2309
Product: qcn6132					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2310
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2311
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	H-QUA-QCN6-260623/2312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2313
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN6-260623/2314
Product: qcn7605					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN7-260623/2315
Product: qcn7606					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN7-260623/2316
Product: qcn9000					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2317
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2318
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2319
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2320
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2321
Product: qcn9001					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/product-	H-QUA-QCN9-260623/2322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2323
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2324
Product: qcn9002					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2325
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2326
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCN9-260623/2327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Product: qcn9003					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2328
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2329
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2330
Product: qcn9011					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2331
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCN9-260623/2332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2333
Product: qcn9012					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2334
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2335
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2336
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2337
Product: qcn9022					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2338
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2339
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2340
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2341
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2342
Product: qcn9024					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2343
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2344
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2345
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2346
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2347
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCN9-260623/2348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21660	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2349
Product: qcn9070					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2350
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2351
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2352
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2354
Product: qcn9072					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2355
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2356
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2357
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2358
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon	https://www.qualcomm.com/company/product-	H-QUA-QCN9-260623/2359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or probe-response frame. **CVE ID : CVE-2023-21661**	security/bulletins/june-2023-bulletin	
Product: qcn9074					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2360
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2361
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2362
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2363
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCN9-260623/2364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21660	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2365
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2366
Product: qcn9100					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2367
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2368
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2370
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2371
Product: qcn9274					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2372
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2373
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCN9-260623/2374
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame.	https://www.qualcomm.com/company/product-	H-QUA-QCN9-260623/2375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21661	security/bulletins/june-2023-bulletin	
Product: qcs2290					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS2-260623/2376
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS2-260623/2377
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS2-260623/2378
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS2-260623/2379
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address.	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS2-260623/2380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21669		
Product: qcs400					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS4-260623/2381
Product: qcs410					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS4-260623/2382
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS4-260623/2383
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS4-260623/2384
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCS4-260623/2385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS4-260623/2386
Product: qcs4290					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS4-260623/2387
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS4-260623/2388
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS4-260623/2389
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS4-260623/2390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS4-260623/2391
Product: qcs4490					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS4-260623/2392
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS4-260623/2393
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS4-260623/2394
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS4-260623/2395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS4-260623/2396
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS4-260623/2397
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS4-260623/2398
Product: qcs605					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS6-260623/2399
Product: qcs610					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS6-260623/2400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS6-260623/2401
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS6-260623/2402
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS6-260623/2403
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS6-260623/2404
Product: qcs6125					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS6-260623/2405
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	H-QUA-QCS6-260623/2406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Product: qcs6490					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS6-260623/2407
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS6-260623/2408
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS6-260623/2409
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS6-260623/2410
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCS6-260623/2411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS6-260623/2412
Product: qcs8155					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS8-260623/2413
Product: qcs8250					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS8-260623/2414
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS8-260623/2415
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCS8-260623/2416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS8-260623/2417
Product: qcs8550					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS8-260623/2418
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS8-260623/2419
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS8-260623/2420
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS8-260623/2421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS8-260623/2422
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS8-260623/2423
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QCS8-260623/2424
Product: qfe1922					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QFE1-260623/2425
Product: qfe1952					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QFE1-260623/2426
Product: qm215					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QM21-260623/2427
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QM21-260623/2428
Product: qrb5165					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QRB5-260623/2429
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QRB5-260623/2430
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QRB5-260623/2431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QRB5-260623/2432
Product: qrb5165m					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QRB5-260623/2433
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QRB5-260623/2434
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QRB5-260623/2435
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QRB5-260623/2436
Product: qrb5165n					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QRB5-260623/2437
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QRB5-260623/2438
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QRB5-260623/2439
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QRB5-260623/2440
Product: qsm8250					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QSM8-260623/2441
Product: qsm8350					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QSM8-260623/2442
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QSM8-260623/2443
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-QSM8-260623/2444
Product: robotics_rb3_platform					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-ROBO-260623/2445
Product: sa4150p					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SA41-260623/2446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA41-260623/2447
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA41-260623/2448
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA41-260623/2449
Product: sa4155p					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA41-260623/2450
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA41-260623/2451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA41-260623/2452
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA41-260623/2453
Product: sa6145p					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2454
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2455
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2456
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case.	https://www.qualcomm.com/company/product-	H-QUA-SA61-260623/2457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21657	security/bulletins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2458
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2459
Product: sa6150p					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2460
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2461
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2463
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2464
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2465
Product: sa6155					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2466
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2467
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while	https://www.qualcomm.com/company/product-	H-QUA-SA61-260623/2468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	security/bulletins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2469
Product: sa6155p					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2470
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2471
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2472
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SA61-260623/2473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2474
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA61-260623/2475
Product: sa8145p					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2476
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2477
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2479
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2480
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2481
Product: sa8150p					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2482
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2483
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while	https://www.qualcomm.com/company/product-	H-QUA-SA81-260623/2484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	security/bulletins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2485
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2486
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2487
Product: sa8155					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2488
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SA81-260623/2489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2490
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2491
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2492
Product: sa8155p					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2493
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2495
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2496
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2497
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2498
Product: sa8195p					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2499
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while	https://www.qualcomm.com/company/product-	H-QUA-SA81-260623/2500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			querying a gsl memory node. **CVE ID : CVE-2023-21632**	security/bulletins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2501
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2502
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2503
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA81-260623/2504
Product: sa8255p					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SA82-260623/2505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA82-260623/2506
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA82-260623/2507
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA82-260623/2508
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA82-260623/2509
Product: sa8295p					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA82-260623/2510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA82-260623/2511
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA82-260623/2512
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA82-260623/2513
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA82-260623/2514
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA82-260623/2515
Product: sa8540p					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while	https://www.qualcomm.com/company/product-	H-QUA-SA85-260623/2516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			querying a gsl memory node. **CVE ID : CVE-2023-21632**	security/bulletins/june-2023-bulletin	
Product: sa9000p					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SA90-260623/2517
Product: sc7180-ac					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC71-260623/2518
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC71-260623/2519
Product: sc7180-ad					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC71-260623/2520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC71-260623/2521
Product: sc8180x-aa					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2522
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2523
Product: sc8180x-ab					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2524
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sc8180x-ac					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2526
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2527
Product: sc8180x-ad					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2528
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2529
Product: sc8180x-af					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SC81-260623/2530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2531
Product: sc8180xp-aa					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2532
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2533
Product: sc8180xp-ab					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2534
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SC81-260623/2535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Product: sc8180xp-ac					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2536
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2537
Product: sc8180xp-ad					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2538
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2539
Product: sc8180xp-af					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2540
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2541
Product: sc8180x\+sdx55					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2542
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC81-260623/2543
Product: sc8280xp-ab					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC82-260623/2544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC82-260623/2545
Product: sc8280xp-bb					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC82-260623/2546
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SC82-260623/2547
Product: sd460					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD46-260623/2548
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD46-260623/2549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sd660					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD66-260623/2550
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD66-260623/2551
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD66-260623/2552
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD66-260623/2553
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD66-260623/2554
Product: sd662					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD66-260623/2555
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD66-260623/2556
Product: sd670					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD67-260623/2557
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD67-260623/2558
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD67-260623/2559
Product: sd675					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD67-260623/2560
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD67-260623/2561
Product: sd730					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD73-260623/2562
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD73-260623/2563
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD73-260623/2564
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending	https://www.qualcomm.com/company/	H-QUA-SD73-260623/2565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	product-security/bulletins/june-2023-bulletin	
Product: sd820					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD82-260623/2566
Product: sd821					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD82-260623/2567
Product: sd835					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD83-260623/2568
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD83-260623/2569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD83-260623/2570
Product: sd855					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD85-260623/2571
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD85-260623/2572
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD85-260623/2573
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD85-260623/2574
Product: sd865_5g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD86-260623/2575
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD86-260623/2576
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD86-260623/2577
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD86-260623/2578
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD86-260623/2579
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SD86-260623/2580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD86-260623/2581
Product: sd888					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD88-260623/2582
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD88-260623/2583
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD88-260623/2584
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD88-260623/2585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD88-260623/2586
Product: sda845					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDA8-260623/2587
Product: sdm429					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM4-260623/2588
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM4-260623/2589
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM4-260623/2590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM4-260623/2591
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM4-260623/2592
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM4-260623/2593
Product: sdm429w					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM4-260623/2594
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM4-260623/2595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM4-260623/2596
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM4-260623/2597
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM4-260623/2598
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM4-260623/2599
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM4-260623/2600
Product: sdm439					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM4-260623/2601
Product: sdm660					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM6-260623/2602
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM6-260623/2603
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM6-260623/2604
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM6-260623/2605
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon	https://www.qualcomm.com/company/product-	H-QUA-SDM6-260623/2606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or probe-response frame. **CVE ID : CVE-2023-21661**	security/bulletins/june-2023-bulletin	
Product: sdm670					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM6-260623/2607
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM6-260623/2608
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM6-260623/2609
Product: sdm710					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM7-260623/2610
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command	https://www.qualcomm.com/company/	H-QUA-SDM7-260623/2611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	product-security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM7-260623/2612
Product: sdm712					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM7-260623/2613
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM7-260623/2614
Product: sdm845					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDM8-260623/2615
Product: sdx20m					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDX2-260623/2616
Product: sdx55					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDX5-260623/2617
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDX5-260623/2618
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDX5-260623/2619
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SDX5-260623/2620
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending	https://www.qualcomm.com/company/	H-QUA-SDX5-260623/2621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	product-security/bulletins/june-2023-bulletin	
Product: sd_455					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD_4-260623/2622
Product: sd_675					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD_6-260623/2623
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD_6-260623/2624
Product: sd_8cx					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD_8-260623/2625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628		
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD_8-260623/2626
Product: sd_8_gen1_5g					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD_8-260623/2627
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SD_8-260623/2628
Product: sg4150p					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SG41-260623/2629
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SG41-260623/2630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21657	tins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SG41-260623/2631
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SG41-260623/2632
Product: sm4125					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM41-260623/2633
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM41-260623/2634
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM41-260623/2635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM41-260623/2636
Product: sm4250-aa					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM42-260623/2637
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM42-260623/2638
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM42-260623/2639
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM42-260623/2640
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	H-QUA-SM42-260623/2641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Product: sm4350					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM43-260623/2642
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM43-260623/2643
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM43-260623/2644
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM43-260623/2645
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SM43-260623/2646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Product: sm4350-ac					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM43-260623/2647
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM43-260623/2648
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM43-260623/2649
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM43-260623/2650
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM43-260623/2651
Product: sm4375					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM43-260623/2652
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM43-260623/2653
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM43-260623/2654
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM43-260623/2655
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM43-260623/2656
Product: sm4450					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM44-260623/2657
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM44-260623/2658
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM44-260623/2659
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM44-260623/2660
Product: sm6125					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM61-260623/2661
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command	https://www.qualcomm.com/company/	H-QUA-SM61-260623/2662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	product-security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM61-260623/2663
Product: sm6150-ac					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM61-260623/2664
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM61-260623/2665
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM61-260623/2666
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SM61-260623/2667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21669	tins/june-2023-bulletin	
Product: sm6225					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM62-260623/2668
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM62-260623/2669
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM62-260623/2670
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM62-260623/2671
Product: sm6225-ad					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SM62-260623/2672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM62-260623/2673
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM62-260623/2674
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM62-260623/2675
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM62-260623/2676
Product: sm6250					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM62-260623/2677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM62-260623/2678
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM62-260623/2679
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM62-260623/2680
Product: sm6250p					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM62-260623/2681
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM62-260623/2682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM62-260623/2683
Product: sm6350					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM63-260623/2684
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM63-260623/2685
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM63-260623/2686
Product: sm6375					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM63-260623/2687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM63-260623/2688
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM63-260623/2689
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM63-260623/2690
Product: sm7125					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM71-260623/2691
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM71-260623/2692
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	H-QUA-SM71-260623/2693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM71-260623/2694
Product: sm7150-aa					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM71-260623/2695
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM71-260623/2696
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM71-260623/2697
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SM71-260623/2698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			peer with an invalid source address. **CVE ID : CVE-2023-21669**	tins/june-2023-bulletin	
Product: sm7150-ab					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM71-260623/2699
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM71-260623/2700
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM71-260623/2701
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM71-260623/2702
Product: sm7150-ac					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM71-260623/2703
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM71-260623/2704
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM71-260623/2705
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM71-260623/2706
Product: sm7225					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM72-260623/2707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM72-260623/2708
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM72-260623/2709
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM72-260623/2710
Product: sm7250-aa					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM72-260623/2711
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM72-260623/2712
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command	https://www.qualcomm.com/company/product-	H-QUA-SM72-260623/2713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM72-260623/2714
Product: sm7250-ab					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM72-260623/2715
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM72-260623/2716
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM72-260623/2717
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SM72-260623/2718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Product: sm7250-ac					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM72-260623/2719
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM72-260623/2720
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM72-260623/2721
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM72-260623/2722
Product: sm7250p					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SM72-260623/2723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM72-260623/2724
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM72-260623/2725
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM72-260623/2726
Product: sm7315					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2727
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2729
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2730
Product: sm7325					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2731
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2732
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2733
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	H-QUA-SM73-260623/2734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Product: sm7325-ae					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2735
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2736
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2737
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2738
Product: sm7325-af					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware.	https://www.qualcomm.com/company/product-	H-QUA-SM73-260623/2739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21656	security/bulletins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2740
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2741
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2742
Product: sm7325p					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2743
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2745
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2746
Product: sm7350-ab					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2747
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2748
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2749
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/product-	H-QUA-SM73-260623/2750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM73-260623/2751
Product: sm8150					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM81-260623/2752
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM81-260623/2753
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM81-260623/2754
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SM81-260623/2755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21669	tins/june-2023-bulletin	
Product: sm8150-ac					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM81-260623/2756
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM81-260623/2757
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM81-260623/2758
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM81-260623/2759
Product: sm8250					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SM82-260623/2760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21656	tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2761
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2762
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2763
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2764
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2765
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to	https://www.qualcomm.com/company/product-	H-QUA-SM82-260623/2766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			peer with an invalid source address. **CVE ID : CVE-2023-21669**	security/bulletins/june-2023-bulletin	
Product: sm8250-ab					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2767
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2768
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2769
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2770
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SM82-260623/2771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2772
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2773
Product: sm8250-ac					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2774
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2775
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2777
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2778
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2779
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM82-260623/2780
Product: sm8350					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM83-260623/2781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM83-260623/2782
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM83-260623/2783
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM83-260623/2784
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM83-260623/2785
Product: sm8350-ac					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM83-260623/2786
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP	https://www.qualcomm.com/company/product-	H-QUA-SM83-260623/2787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sends input during record use case. **CVE ID : CVE-2023-21657**	security/bulletins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM83-260623/2788
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM83-260623/2789
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM83-260623/2790
Product: sm8450					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM84-260623/2791
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SM84-260623/2792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM84-260623/2793
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM84-260623/2794
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM84-260623/2795
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM84-260623/2796
Product: sm8475					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM84-260623/2797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM84-260623/2798
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM84-260623/2799
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM84-260623/2800
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SM84-260623/2801
Product: smart_audio_200_platform					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SMAR-260623/2802
Product: smart_audio_400_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SMAR-260623/2803
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SMAR-260623/2804
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SMAR-260623/2805
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SMAR-260623/2806
Product: snapdragonwear_4100\+_platform					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2807
Product: snapdragon_210_processor					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2808
Product: snapdragon_212_mobile_platform					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2809
Product: snapdragon_630_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2810
Product: snapdragon_636_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2811
Product: snapdragon_652_mobile_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2812
Product: snapdragon_662_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2813
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2814
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2815
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2816
Product: snapdragon_675_mobile_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2817
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2818
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2819
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2820
Product: snapdragon_680_4g_mobile_platform					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2821
Product: snapdragon_690_5g_mobile_platform					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2822
Product: snapdragon_695_5g_mobile_platform					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2823
Product: snapdragon_7c\+_gen3_compute					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2824
Product: snapdragon_7c\+_gen_3_compute					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2825
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case.	https://www.qualcomm.com/company/product-	H-QUA-SNAP-260623/2826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21657	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2827
Product: snapdragon_808_processor					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2828
Product: snapdragon_810_processor					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2829
Product: snapdragon_820_automotive_platform					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2831
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2832
Product: snapdragon_820_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2833
Product: snapdragon_821_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2834
Product: snapdragon_835_mobile_pc_platform					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SNAP-260623/2835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2836
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2837
Product: snapdragon_845_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2838
Product: snapdragon_850_mobile_compute_platform					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2839
Product: snapdragon_ar2_gen1_platform					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command	https://www.qualcomm.com/company/	H-QUA-SNAP-260623/2840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	product-security/bulletins/june-2023-bulletin	
Product: snapdragon_ar2_gen_1_platform					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2841
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2842
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2843
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2844
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SNAP-260623/2845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Product: snapdragon_auto_4g_modem					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2846
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2847
Product: snapdragon_auto_5g_modem-rf					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2848
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2849
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SNAP-260623/2850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2851
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2852
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2853
Product: snapdragon_w5\+_gen1_wearable_platform					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2854
Product: snapdragon_w5\+_gen_1_wearable_platform					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SNAP-260623/2855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2856
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2857
Product: snapdragon_x12_lte_modem					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2858
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2859
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2860
Product: snapdragon_x20_lte_modem					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2861
Product: snapdragon_x24_lte_modem					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2862
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2863
Product: snapdragon_x50_5g_modem-rf_system					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2864
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SNAP-260623/2865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2866
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2867
Product: snapdragon_x55_5g_modem-rf_system					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2868
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2869
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2871
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2872
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2873
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2874
Product: snapdragon_x5_lte_modem					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2875
Product: snapdragon_x65_5g_modem-rf_system					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2876
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2877
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2878
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2879
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2880
Product: snapdragon_xr1_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2881
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2882
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2883
Product: snapdragon_xr2\+_gen1_platform					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2884
Product: snapdragon_xr2\+_gen_1_platform					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2886
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2887
Product: snapdragon_xr2_5g_platform					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2888
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2889
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2890
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/product-	H-QUA-SNAP-260623/2891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2892
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2893
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SNAP-260623/2894
Product: ssg2115p					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SSG2-260623/2895
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SSG2-260623/2896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SSG2-260623/2897
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SSG2-260623/2898
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SSG2-260623/2899
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SSG2-260623/2900
Product: ssg2125p					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SSG2-260623/2901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SSG2-260623/2902
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SSG2-260623/2903
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SSG2-260623/2904
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SSG2-260623/2905
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SSG2-260623/2906
Product: sw5100					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF	https://www.qualcomm.com/company/product-	H-QUA-SW51-260623/2907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	security/bulletins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SW51-260623/2908
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SW51-260623/2909
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SW51-260623/2910
Product: sw5100p					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SW51-260623/2911
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SW51-260623/2912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SW51-260623/2913
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SW51-260623/2914
Product: sxr1120					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR1-260623/2915
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR1-260623/2916
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR1-260623/2917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sxr1230p					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR1-260623/2918
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR1-260623/2919
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR1-260623/2920
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR1-260623/2921
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR1-260623/2922
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon	https://www.qualcomm.com/company/product-	H-QUA-SXR1-260623/2923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or probe-response frame. **CVE ID : CVE-2023-21661**	security/bulletins/june-2023-bulletin	
Product: sxr2130					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR2-260623/2924
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR2-260623/2925
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR2-260623/2926
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR2-260623/2927
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SXR2-260623/2928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR2-260623/2929
Product: sxr2230p					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR2-260623/2930
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR2-260623/2931
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR2-260623/2932
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR2-260623/2933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR2-260623/2934
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-SXR2-260623/2935
Product: vision_intelligence_300_platform					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-VISI-260623/2936
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-VISI-260623/2937
Product: vision_intelligence_400_platform					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-VISI-260623/2938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-VISI-260623/2939
Product: wcd9326					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2940
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2941
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2942
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2943
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	H-QUA-WCD9-260623/2944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Product: wcd9330					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2945
Product: wcd9335					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2946
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2947
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2948
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command	https://www.qualcomm.com/company/product-	H-QUA-WCD9-260623/2949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2950
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2951
Product: wcd9340					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2952
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2953
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCD9-260623/2954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21657	tins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2955
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2956
Product: wcd9341					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2957
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2958
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2960
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2961
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2962
Product: wcd9360					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2963
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2964
Product: wcd9370					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2965
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2966
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2967
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2968
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2969
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCD9-260623/2970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2971
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2972
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2973
Product: wcd9371					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2974
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wcd9375					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2976
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2977
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2978
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2979
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2980
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	H-QUA-WCD9-260623/2981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2982
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2983
Product: wcd9380					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2984
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2985
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCD9-260623/2986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21657	tins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2987
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2988
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2989
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2990
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2991
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to	https://www.qualcomm.com/company/product-	H-QUA-WCD9-260623/2992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			peer with an invalid source address. **CVE ID : CVE-2023-21669**	security/bulletins/june-2023-bulletin	
Product: wcd9385					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2993
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2994
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2995
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2996
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCD9-260623/2997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21658	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2998
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/2999
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/3000
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCD9-260623/3001
Product: wcn3610					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3003
Product: wcn3615					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3004
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3005
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3006
Product: wcn3620					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3008
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3009
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3010
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3011
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3012
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCN3-260623/3013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21669	tins/june-2023-bulletin	
Product: wcn3660b					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3014
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3015
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3016
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3017
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3019
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3020
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3021
Product: wcn3680					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3022
Product: wcn3680b					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3024
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3025
Product: wcn3910					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3026
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3027
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3028
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	H-QUA-WCN3-260623/3029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3030
Product: wcn3950					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3031
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3032
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3033
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCN3-260623/3034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3035
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3036
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3037
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3038
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3039
Product: wcn3980					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3040
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3041
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3042
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3043
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3044
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCN3-260623/3045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21669	tins/june-2023-bulletin	
Product: wcn3988					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3046
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3047
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3048
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3049
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3051
Product: wcn3990					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3052
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3053
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3054
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3056
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3057
Product: wcn3991					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3058
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3059
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3061
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3062
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3063
Product: wcn3998					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3064
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3066
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3067
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3068
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3069
Product: wcn3999					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN3-260623/3070
Product: wcn6740					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3071
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3072
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3073
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3074
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3075
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCN6-260623/3076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Product: wcn6750					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3077
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3078
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3079
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3080
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3082
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3083
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3084
Product: wcn685x-1					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3085
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3086
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case.	https://www.qualcomm.com/company/product-	H-QUA-WCN6-260623/3087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21657	security/bulletins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3088
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3089
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3090
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3091
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3092
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending	https://www.qualcomm.com/company/	H-QUA-WCN6-260623/3093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	product-security/bulletins/june-2023-bulletin	
Product: wcn685x-5					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3094
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3095
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3096
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3097
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCN6-260623/3098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21658	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3099
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3100
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3101
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN6-260623/3102
Product: wcn785x-1					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN7-260623/3103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN7-260623/3104
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN7-260623/3105
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN7-260623/3106
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN7-260623/3107
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN7-260623/3108
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCN7-260623/3109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Product: wcn785x-5					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN7-260623/3110
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN7-260623/3111
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN7-260623/3112
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN7-260623/3113
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN7-260623/3114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN7-260623/3115
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WCN7-260623/3116
Product: wsa8810					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3117
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3118
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3119
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command	https://www.qualcomm.com/company/product-	H-QUA-WSA8-260623/3120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3121
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3122
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3123
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3124
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wsa8815					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3126
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3127
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3128
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3129
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3130
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	H-QUA-WSA8-260623/3131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3132
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3133
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3134
Product: wsa8830					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3135
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WSA8-260623/3136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21656	tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3137
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3138
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3139
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3140
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3141
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame.	https://www.qualcomm.com/company/product-	H-QUA-WSA8-260623/3142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21661	security/bulletins/june-2023-bulletin	
Product: wsa8832					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3143
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3144
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3145
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3146
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3148
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3149
Product: wsa8835					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3150
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3151
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3152
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command	https://www.qualcomm.com/company/product-	H-QUA-WSA8-260623/3153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3154
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3155
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3156
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	H-QUA-WSA8-260623/3157
Vendor: Samsung					
Product: exynos_5123					
Affected Version(s): -					
Incorrect Default Permissions	07-Jun-2023	9.8	An issue was discovered in the Shannon RCS component in Samsung Exynos	https://semiconductor.samsung.com/support/quality-support/prod	H-SAM-EXYN-260623/3158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem 5123 and 5300. An incorrect default permission can cause unintended querying of RCS capability via a crafted application. **CVE ID : CVE-2023-31116**	uct-security-updates/	
Incorrect Resource Transfer Between Spheres	07-Jun-2023	9.1	An issue was discovered in the Shannon RCS component in Samsung Exynos Modem 5123 and 5300. Incorrect resource transfer between spheres can cause unintended querying of the SIM status via a crafted application. **CVE ID : CVE-2023-31114**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-260623/3159
Incorrect Resource Transfer Between Spheres	07-Jun-2023	7.5	An issue was discovered in the Shannon RCS component in Samsung Exynos Modem 5123 and 5300. Incorrect resource transfer between spheres can cause changes to the activation mode of RCS via a crafted application. **CVE ID : CVE-2023-31115**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-260623/3160
Product: exynos_5300					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	07-Jun-2023	9.8	An issue was discovered in the Shannon RCS component in Samsung Exynos Modem 5123 and 5300. An incorrect default permission can cause unintended querying of RCS capability via a crafted application. **CVE ID : CVE-2023-31116**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-260623/3161
Incorrect Resource Transfer Between Spheres	07-Jun-2023	9.1	An issue was discovered in the Shannon RCS component in Samsung Exynos Modem 5123 and 5300. Incorrect resource transfer between spheres can cause unintended querying of the SIM status via a crafted application. **CVE ID : CVE-2023-31114**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-260623/3162
Incorrect Resource Transfer Between Spheres	07-Jun-2023	7.5	An issue was discovered in the Shannon RCS component in Samsung Exynos Modem 5123 and 5300. Incorrect resource transfer between spheres can cause changes to the activation mode of RCS via a crafted application.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-260623/3163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31115		
Vendor: telefonica					
Product: brasil_vivo_play					
Affected Version(s): -					
Uncontrolled Recursion	05-Jun-2023	7.5	Telefnica Brasil Vivo Play (IPTV) Firmware: 2023.04.04.01.06.15 is vulnerable to Denial of Service (DoS) via DNS Recursion. **CVE ID : CVE-2023-31893**	N/A	H-TEL-BRAS-260623/3164
Vendor: Tenda					
Product: ac10					
Affected Version(s): 4.0					
Out-of-bounds Write	08-Jun-2023	9.8	Tenda AC10 v4 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via parameter time at /goform/saveParentControlInfo. **CVE ID : CVE-2023-34566**	N/A	H-TEN-AC10-260623/3165
Out-of-bounds Write	08-Jun-2023	6.7	Tenda AC10 v4 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via parameter list at /goform/SetVirtualServerCfg. **CVE ID : CVE-2023-34567**	N/A	H-TEN-AC10-260623/3166
Out-of-bounds Write	08-Jun-2023	6.7	Tenda AC10 v4 US_AC10V4.0si_V16.03.10.13_cn was	N/A	H-TEN-AC10-260623/3167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a stack overflow via parameter time at /goform/PowerSaveSet. **CVE ID : CVE-2023-34568**		
Out-of-bounds Write	08-Jun-2023	6.7	Tenda AC10 v4 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via parameter list at /goform/SetNetControlList. **CVE ID : CVE-2023-34569**	N/A	H-TEN-AC10-260623/3168
Out-of-bounds Write	08-Jun-2023	6.7	Tenda AC10 v4 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via parameter devName at /goform/SetOnlineDevName. **CVE ID : CVE-2023-34570**	N/A	H-TEN-AC10-260623/3169
Out-of-bounds Write	08-Jun-2023	6.7	Tenda AC10 v4 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via parameter shareSpeed at /goform/WifiGuestSet. **CVE ID : CVE-2023-34571**	N/A	H-TEN-AC10-260623/3170
Product: ac8					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jun-2023	9.8	Tenda AC8V4.0-V16.03.34.06 was discovered to contain a stack overflow via the timeZone parameter in the sub_44db3c function. **CVE ID : CVE-2023-33669**	N/A	H-TEN-AC8-260623/3171
Out-of-bounds Write	02-Jun-2023	9.8	Tenda AC8V4.0-V16.03.34.06 was discovered to contain a stack overflow via the time parameter in the sub_4a79ec function. **CVE ID : CVE-2023-33670**	N/A	H-TEN-AC8-260623/3172
Out-of-bounds Write	02-Jun-2023	9.8	Tenda AC8V4.0-V16.03.34.06 was discovered to contain a stack overflow via the deviceId parameter in the saveParentControlInfo function. **CVE ID : CVE-2023-33671**	N/A	H-TEN-AC8-260623/3173
Out-of-bounds Write	02-Jun-2023	9.8	Tenda AC8V4.0-V16.03.34.06 was discovered to contain a stack overflow via the firewallEn parameter in the formSetFirewallCfg function. **CVE ID : CVE-2023-33673**	N/A	H-TEN-AC8-260623/3174
Out-of-bounds Write	02-Jun-2023	9.8	Tenda AC8V4.0-V16.03.34.06 was discovered to contain	N/A	H-TEN-AC8-260623/3175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a stack overflow via the time parameter in the get_parentControl_list_Info function. **CVE ID : CVE-2023-33675**		
Out-of-bounds Write	02-Jun-2023	7.5	Tenda AC8V4.0-V16.03.34.06 was discovered to contain a stack overflow via the shareSpeed parameter in the fromSetWifiGusetBasic function. **CVE ID : CVE-2023-33672**	N/A	H-TEN-AC8-260623/3176
Product: g103					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jun-2023	8.8	There is a command injection vulnerability in the Tenda G103 Gigabit GPON Terminal with firmware version V1.0.0.5. If an attacker gains web management privileges, they can inject commands gaining shell privileges. **CVE ID : CVE-2023-33530**	N/A	H-TEN-G103-260623/3177
Vendor: totolink					
Product: a7100ru					
Affected Version(s): -					
Improper Neutralization of	07-Jun-2023	9.8	TOTOLink A7100RU V7.4cu.2313_B20191024 was discovered to	N/A	H-TOT-A710-260623/3178

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 staticGw parameter at /setting/setWanIeCfg. **CVE ID : CVE-2023-33556**		
Product: x5000r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jun-2023	9.8	TOTOLINK X5000R V9.1.0cu.2350_B20230313 was discovered to contain a command injection via the setWanCfg function. **CVE ID : CVE-2023-31569**	N/A	H-TOT-X500-260623/3179
Vendor: Tp-link					
Product: tapo_c200					
Affected Version(s): 3					
Insufficiently Protected Credentials	06-Jun-2023	4.6	The AES Key-IV pair used by the TP-Link TAPO C200 camera V3 (EU) on firmware version 1.1.22 Build 220725 is reused across all cameras. An attacker with physical access to a camera is able to extract and decrypt sensitive data containing the Wifi password and the TP-LINK account credential of the victim. **CVE ID : CVE-2023-27126**	N/A	H-TP--TAPO-260623/3180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: tl-wr740n					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jun-2023	8.8	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a command injection vulnerability via the component /userRpm/WlanNetworkRpm . **CVE ID : CVE-2023-33538**	N/A	H-TP--TL-W-260623/3181
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/WlanMacFilterRpm. **CVE ID : CVE-2023-33536**	N/A	H-TP--TL-W-260623/3182
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/FixMapCfgRpm. **CVE ID : CVE-2023-33537**	N/A	H-TP--TL-W-260623/3183
Affected Version(s): 2.0					
Improper Neutralization of Special	07-Jun-2023	8.8	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was	N/A	H-TP--TL-W-260623/3184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			discovered to contain a command injection vulnerability via the component /userRpm/WlanNetworkRpm . **CVE ID : CVE-2023-33538**		
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/WlanMacFilterRpm. **CVE ID : CVE-2023-33536**	N/A	H-TP--TL-W-260623/3185
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/FixMapCfgRpm. **CVE ID : CVE-2023-33537**	N/A	H-TP--TL-W-260623/3186
Product: tl-wr841n					
Affected Version(s): 10.0					
Improper Neutralization of Special Elements used in a Command ('Comman	07-Jun-2023	8.8	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a command injection vulnerability via the component	N/A	H-TP--TL-W-260623/3187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			/userRpm/WlanNetworkRpm . **CVE ID : CVE-2023-33538**		
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/WlanMacFilterRpm. **CVE ID : CVE-2023-33536**	N/A	H-TP--TL-W-260623/3188
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/FixMapCfgRpm. **CVE ID : CVE-2023-33537**	N/A	H-TP--TL-W-260623/3189
Affected Version(s): 8.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jun-2023	8.8	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a command injection vulnerability via the component /userRpm/WlanNetworkRpm . **CVE ID : CVE-2023-33538**	N/A	H-TP--TL-W-260623/3190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/WlanMacFilterRpm. **CVE ID : CVE-2023-33536**	N/A	H-TP--TL-W-260623/3191
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/FixMapCfgRpm. **CVE ID : CVE-2023-33537**	N/A	H-TP--TL-W-260623/3192
Product: tl-wr940n					
Affected Version(s): 4.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jun-2023	8.8	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a command injection vulnerability via the component /userRpm/WlanNetworkRpm . **CVE ID : CVE-2023-33538**	N/A	H-TP--TL-W-260623/3193
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain	N/A	H-TP--TL-W-260623/3194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a buffer overflow via the component /userRpm/WlanMacFilterRpm. **CVE ID : CVE-2023-33536**		
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/FixMapCfgRpm. **CVE ID : CVE-2023-33537**	N/A	H-TP--TL-W-260623/3195
Affected Version(s): 2.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jun-2023	8.8	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a command injection vulnerability via the component /userRpm/WlanNetworkRpm . **CVE ID : CVE-2023-33538**	N/A	H-TP--TL-W-260623/3196
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/WlanMacFilterRpm. **CVE ID : CVE-2023-33536**	N/A	H-TP--TL-W-260623/3197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/FixMapCfgRpm. **CVE ID : CVE-2023-33537**	N/A	H-TP--TL-W-260623/3198
Vendor: unisoc					
Product: s8000					
Affected Version(s): -					
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30863**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624798	H-UNI-S800-260623/3199
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30864**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624798	H-UNI-S800-260623/3200
Missing Authorization	06-Jun-2023	5.5	In dialer service, there is a missing permission check. This could lead to local information	https://www.unisoc.com/en_us/secy/announcementDetail/166482	H-UNI-S800-260623/3201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30865**	23614147624 98	
Missing Authorization	06-Jun-2023	5.5	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30866**	https://www.unisoc.com/en_us/secy/announcementDetail/166482 23614147624 98	H-UNI-S800-260623/3202
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30914**	https://www.unisoc.com/en_us/secy/announcementDetail/166482 23614147624 98	H-UNI-S800-260623/3203
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30915**	https://www.unisoc.com/en_us/secy/announcementDetail/166482 23614147624 98	H-UNI-S800-260623/3204
Product: sc7731e					
Affected Version(s): -					
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check.	https://www.unisoc.com/en_us/secy/announcementD	H-UNI-SC77-260623/3205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30863**	etail/16648223614147624998	
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30864**	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624998	H-UNI-SC77-260623/3206
Missing Authorization	06-Jun-2023	5.5	In dialer service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30865**	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624998	H-UNI-SC77-260623/3207
Missing Authorization	06-Jun-2023	5.5	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30866**	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624998	H-UNI-SC77-260623/3208
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check.	https://www.unisoc.com/en_us/secy/an	H-UNI-SC77-260623/3209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30914**	nouncementDetail/166482236141476249 8	
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30915**	https://www.unisoc.com/en_us/secy/announcementDetail/166482236141476249 8	H-UNI-SC77-260623/3210
Product: sc9832e					
Affected Version(s): -					
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30863**	https://www.unisoc.com/en_us/secy/announcementDetail/166482236141476249 8	H-UNI-SC98-260623/3211
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30864**	https://www.unisoc.com/en_us/secy/announcementDetail/166482236141476249 8	H-UNI-SC98-260623/3212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jun-2023	5.5	In dialer service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30865**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-SC98-260623/3213
Missing Authorization	06-Jun-2023	5.5	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30866**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-SC98-260623/3214
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30914**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-SC98-260623/3215
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30915**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-SC98-260623/3216
Product: sc9863a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30863**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-SC98-260623/3217
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30864**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-SC98-260623/3218
Missing Authorization	06-Jun-2023	5.5	In dialer service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30865**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-SC98-260623/3219
Missing Authorization	06-Jun-2023	5.5	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-SC98-260623/3220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30866		
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30914**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-SC98-260623/3221
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30915**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-SC98-260623/3222
Product: t310					
Affected Version(s): -					
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30863**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-T310-260623/3223
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of	https://www.unisoc.com/en_us/secy/announcementDetail/166482	H-UNI-T310-260623/3224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges. **CVE ID : CVE-2023-30864**	2361414762498	
Missing Authorization	06-Jun-2023	5.5	In dialer service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30865**	https://www.unisoc.com/en_us/secy/announcementDetail/1664822361414762498	H-UNI-T310-260623/3225
Missing Authorization	06-Jun-2023	5.5	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30866**	https://www.unisoc.com/en_us/secy/announcementDetail/1664822361414762498	H-UNI-T310-260623/3226
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30914**	https://www.unisoc.com/en_us/secy/announcementDetail/1664822361414762498	H-UNI-T310-260623/3227
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no	https://www.unisoc.com/en_us/secy/announcementDetail/166482	H-UNI-T310-260623/3228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. **CVE ID : CVE-2023-30915**	23614147624 98	
Product: t606					
Affected Version(s): -					
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30863**	https://www.unisoc.com/en_us/secy/announcementDetail/166482 23614147624 98	H-UNI-T606-260623/3229
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30864**	https://www.unisoc.com/en_us/secy/announcementDetail/166482 23614147624 98	H-UNI-T606-260623/3230
Missing Authorization	06-Jun-2023	5.5	In dialer service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30865**	https://www.unisoc.com/en_us/secy/announcementDetail/166482 23614147624 98	H-UNI-T606-260623/3231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jun-2023	5.5	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30866**	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624998	H-UNI-T606-260623/3232
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30914**	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624998	H-UNI-T606-260623/3233
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30915**	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624998	H-UNI-T606-260623/3234
Product: t610					
Affected Version(s): -					
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624998	H-UNI-T610-260623/3235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30863		
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30864**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624798	H-UNI-T610-260623/3236
Missing Authorization	06-Jun-2023	5.5	In dialer service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30865**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624798	H-UNI-T610-260623/3237
Missing Authorization	06-Jun-2023	5.5	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30866**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624798	H-UNI-T610-260623/3238
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624798	H-UNI-T610-260623/3239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30914		
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30915**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-T610-260623/3240
Product: t612					
Affected Version(s): -					
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30863**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-T612-260623/3241
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30864**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-T612-260623/3242
Missing Authorization	06-Jun-2023	5.5	In dialer service, there is a missing permission check. This could lead to local information	https://www.unisoc.com/en_us/secy/announcementDetail/166482	H-UNI-T612-260623/3243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30865**	23614147624 98	
Missing Authorization	06-Jun-2023	5.5	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30866**	https://www.unisoc.com/en_us/secy/announcementDetail/166482 23614147624 98	H-UNI-T612-260623/3244
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30914**	https://www.unisoc.com/en_us/secy/announcementDetail/166482 23614147624 98	H-UNI-T612-260623/3245
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30915**	https://www.unisoc.com/en_us/secy/announcementDetail/166482 23614147624 98	H-UNI-T612-260623/3246
Product: t616					
Affected Version(s): -					
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check.	https://www.unisoc.com/en_us/secy/announcementD	H-UNI-T616-260623/3247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30863**	etail/16648223614147624998	
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30864**	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624998	H-UNI-T616-260623/3248
Missing Authorization	06-Jun-2023	5.5	In dialer service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30865**	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624998	H-UNI-T616-260623/3249
Missing Authorization	06-Jun-2023	5.5	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30866**	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624998	H-UNI-T616-260623/3250
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check.	https://www.unisoc.com/en_us/secy/an	H-UNI-T616-260623/3251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30914**	nouncementDetail/166482361414762498	
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30915**	https://www.unisoc.com/en_us/secy/announcementDetail/166482361414762498	H-UNI-T616-260623/3252
Product: t618					
Affected Version(s): -					
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30863**	https://www.unisoc.com/en_us/secy/announcementDetail/166482361414762498	H-UNI-T618-260623/3253
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30864**	https://www.unisoc.com/en_us/secy/announcementDetail/166482361414762498	H-UNI-T618-260623/3254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jun-2023	5.5	In dialer service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30865**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-T618-260623/3255
Missing Authorization	06-Jun-2023	5.5	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30866**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-T618-260623/3256
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30914**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-T618-260623/3257
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30915**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-T618-260623/3258
Product: t760					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30863**	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624498	H-UNI-T760-260623/3259
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30864**	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624498	H-UNI-T760-260623/3260
Missing Authorization	06-Jun-2023	5.5	In dialer service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30865**	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624498	H-UNI-T760-260623/3261
Missing Authorization	06-Jun-2023	5.5	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624498	H-UNI-T760-260623/3262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30866		
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30914**	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624498	H-UNI-T760-260623/3263
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30915**	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624498	H-UNI-T760-260623/3264
Product: t770					
Affected Version(s): -					
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30863**	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624498	H-UNI-T770-260623/3265
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of	https://www.unisoc.com/en_us/secy/announcementDetail/166482	H-UNI-T770-260623/3266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges. **CVE ID : CVE-2023-30864**	2361414762498	
Missing Authorization	06-Jun-2023	5.5	In dialer service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30865**	https://www.unisoc.com/en_us/secy/announcementDetail/1664822361414762498	H-UNI-T770-260623/3267
Missing Authorization	06-Jun-2023	5.5	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30866**	https://www.unisoc.com/en_us/secy/announcementDetail/1664822361414762498	H-UNI-T770-260623/3268
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30914**	https://www.unisoc.com/en_us/secy/announcementDetail/1664822361414762498	H-UNI-T770-260623/3269
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no	https://www.unisoc.com/en_us/secy/announcementDetail/166482	H-UNI-T770-260623/3270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. **CVE ID : CVE-2023-30915**	23614147624 98	
Product: t820					
Affected Version(s): -					
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30863**	https://www.unisoc.com/en_us/secy/announcementDetail/166482 23614147624 98	H-UNI-T820-260623/3271
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30864**	https://www.unisoc.com/en_us/secy/announcementDetail/166482 23614147624 98	H-UNI-T820-260623/3272
Missing Authorization	06-Jun-2023	5.5	In dialer service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30865**	https://www.unisoc.com/en_us/secy/announcementDetail/166482 23614147624 98	H-UNI-T820-260623/3273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jun-2023	5.5	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30866**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-T820-260623/3274
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30914**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-T820-260623/3275
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30915**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	H-UNI-T820-260623/3276
Vendor: Zyxel					
Product: lte7480-m804					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	05-Jun-2023	6.5	A buffer overflow vulnerability in the CGI program of the Zyxel NR7101 firmware versions prior to V1.00(ABUV.8)C0 could allow a remote	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-	H-ZYX-LTE7-260623/3277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			authenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID : CVE-2023-27989**	overflow-vulnerability-in-4g-lte-and-5g-nr-outdoor-routers	
Product: lte7490-m904					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jun-2023	6.5	A buffer overflow vulnerability in the CGI program of the Zyxel NR7101 firmware versions prior to V1.00(ABUV.8)C0 could allow a remote authenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID : CVE-2023-27989**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-4g-lte-and-5g-nr-outdoor-routers	H-ZYX-LTE7-260623/3278
Product: nebula_nr7101					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jun-2023	6.5	A buffer overflow vulnerability in the CGI program of the Zyxel NR7101 firmware versions prior to V1.00(ABUV.8)C0 could allow a remote authenticated attacker to cause denial of service (DoS)	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-4g-lte-and-	H-ZYX-NEBU-260623/3279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID : CVE-2023-27989**	5g-nr-outdoor-routers	
Product: nr7101					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jun-2023	6.5	A buffer overflow vulnerability in the CGI program of the Zyxel NR7101 firmware versions prior to V1.00(ABUV.8)C0 could allow a remote authenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID : CVE-2023-27989**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-4g-lte-and-5g-nr-outdoor-routers	H-ZYX-NR71-260623/3280
Operating System					
Vendor: ABB					
Product: aspect-ent-12_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd.	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-ASPE-270623/3281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCo	O-ABB-ASPE-270623/3282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**	de=en&DocumentPartId=&Action=Launch	
Product: aspect-ent-256_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01;	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-ASPE-270623/3283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-ASPE-270623/3284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: aspect-ent-2_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-ASPE-270623/3285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-ASPE-270623/3286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: aspect-ent-96_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-ASPE-270623/3287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&	O-ABB-ASPE-270623/3288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**	Action=Launch	
Product: matrix-11_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB	https://search.abb.com/library/Downloa	O-ABB-MATR-270623/3289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01.	d.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0635		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-MATR-270623/3290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: matrix-216_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-MATR-270623/3291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-MATR-270623/3292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: matrix-232_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-MATR-270623/3293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-MATR-270623/3294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: matrix-264_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&Docu	O-ABB-MATR-270623/3295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**	mentPartId=&Action=Launch	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1.	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-MATR-270623/3296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0636		
Product: matrix-296_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-MATR-270623/3297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-MATR-270623/3298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: nexus-2128-a_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-NEXU-270623/3299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-NEXU-270623/3300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: nexus-2128-f_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&	O-ABB-NEXU-270623/3301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**	Action=Launch	
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on	https://search.abb.com/library/Download.aspx?DocumentID=2CKA0	O-ABB-NEXU-270623/3302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**	00073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nexus-2128-g_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-NEXU-270623/3303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-NEXU-270623/3304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: nexus-2128_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-NEXU-270623/3305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-NEXU-270623/3306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: nexus-264-a_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-NEXU-270623/3307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&	O-ABB-NEXU-270623/3308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**	Action=Launch	
Product: nexus-264-f_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management	https://search.abb.com/lib	O-ABB-NEXU-270623/3309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01.	rary/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0635		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-NEXU-270623/3310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: nexus-264-g_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-NEXU-270623/3311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd.	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-NEXU-270623/3312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: nexus-264_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-NEXU-270623/3313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-NEXU-270623/3314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Product: nexus-3-2128_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403	O-ABB-NEXU-270623/3315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**	&LanguageCode=en&DocumentPartId=&Action=Launch	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1.	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-NEXU-270623/3316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0636		
Product: nexus-3-264_firmware					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.07.01					
N/A	05-Jun-2023	9.8	Improper Privilege Management vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Privilege	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-NEXU-270623/3317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Escalation.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.01; NEXUS Series: from 3.0;0 before 3.07.01; MATRIX Series: from 3.0;0 before 3.07.01. **CVE ID : CVE-2023-0635**		
Improper Input Validation	05-Jun-2023	9.8	Improper Input Validation vulnerability in ABB Ltd. ASPECT®-Enterprise on ASPECT®-Enterprise, Linux (2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021 modules), ABB Ltd. NEXUS Series on NEXUS Series, Linux (2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021 modules), ABB Ltd. MATRIX Series on MATRIX Series, Linux (2CQG100102R1021, 2CQG100103R1021,	https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-NEXU-270623/3318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021 modules) allows Command Injection.This issue affects ASPECT®-Enterprise: from 3.0;0 before 3.07.0; NEXUS Series: from 3.0;0 before 3.07.0; MATRIX Series: from 3.0;0 before 3.07.1. **CVE ID : CVE-2023-0636**		
Vendor: Apple					
Product: macos					
Affected Version(s): -					
Uncontrolled Search Path Element	07-Jun-2023	7.8	A command Injection Vulnerability in TA for mac-OS prior to version 5.7.9 allows local users to place an arbitrary file into the /Library/Trellix/Agent/bin/ folder. The malicious file is executed by running the TA deployment feature located in the System Tree. **CVE ID : CVE-2023-0976**	https://kcm.trellix.com/corporate/index?page=content&id=SB10398	O-APP-MACO-270623/3319
Vendor: Asus					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: rt-ac86u_firmware					
Affected Version(s): 3.0.0.4.386.51255					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Jun-2023	8.8	ASUS RT-AC86U does not filter special characters for parameters in specific web URLs. A remote attacker with normal user privileges can exploit this vulnerability to perform command injection attack to execute arbitrary system commands, disrupt system or terminate service. **CVE ID : CVE-2023-28702**	N/A	O-ASU-RT-A-270623/3320
Out-of-bounds Write	02-Jun-2023	7.2	ASUS RT-AC86U's specific cgi function has a stack-based buffer overflow vulnerability due to insufficient validation for network packet header length. A remote attacker with administrator privileges can exploit this vulnerability to execute arbitrary system commands, disrupt system or terminate service. **CVE ID : CVE-2023-28703**	N/A	O-ASU-RT-A-270623/3321
Vendor: danfoss					
Product: ak-em100_firmware					
Affected Version(s): * Up to (excluding) 2.2.0.12					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Jun-2023	9.8	The Danfoss AK-EM100 web forms allow for SQL injection in the login forms. **CVE ID : CVE-2023-22583**	N/A	O-DAN-AK-E-270623/3322
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Jun-2023	9.8	The Danfoss AK-EM100 web applications allow for OS command injection through the web application parameters. **CVE ID : CVE-2023-25911**	N/A	O-DAN-AK-E-270623/3323
Cleartext Storage of Sensitive Information	11-Jun-2023	7.5	The Danfoss AK-EM100 stores login credentials in cleartext. **CVE ID : CVE-2023-22584**	N/A	O-DAN-AK-E-270623/3324
Exposure of Sensitive Information to an Unauthorized Actor	11-Jun-2023	7.5	The Danfoss AK-EM100 web applications allow for Local File Inclusion in the file parameter. **CVE ID : CVE-2023-22586**	N/A	O-DAN-AK-E-270623/3325
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jun-2023	6.1	The Danfoss AK-EM100 web applications allow for Reflected Cross-Site Scripting. **CVE ID : CVE-2023-22582**	N/A	O-DAN-AK-E-270623/3326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jun-2023	6.1	The Danfoss AK-EM100 web applications allow for Reflected Cross-Site Scripting in the title parameter. **CVE ID : CVE-2023-22585**	N/A	O-DAN-AK-E-270623/3327
Exposure of Sensitive Information to an Unauthorized Actor	11-Jun-2023	5.3	The webreport generation feature in the Danfoss AK-EM100 allows an unauthorized actor to generate a web report that discloses sensitive information such as the internal IP address, usernames and internal device values. **CVE ID : CVE-2023-25912**	N/A	O-DAN-AK-E-270623/3328
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
Out-of-bounds Write	01-Jun-2023	5.5	OpenPrinting CUPS is an open source printing system. In versions 2.4.2 and prior, a heap buffer overflow vulnerability would allow a remote attacker to launch a denial of service (DoS) attack. A buffer overflow vulnerability in the function `format_log_line` could allow remote attackers to cause a DoS on the affected	https://github.com/OpenPrinting/cups/security/advisories/GHSA-cxc6-w2g7-69p7	O-DEB-DEBI-270623/3329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. Exploitation of the vulnerability can be triggered when the configuration file `cupsd.conf` sets the value of `loglevel `to `DEBUG`. No known patches or workarounds exist at time of publication. **CVE ID : CVE-2023-32324**		
Missing Release of Memory after Effective Lifetime	06-Jun-2023	3.3	A vulnerability was found in the pthread_create() function in libcap. This issue may allow a malicious actor to use cause __real_pthread_create( ) to return an error, which can exhaust the process memory. **CVE ID : CVE-2023-2602**	N/A	O-DEB-DEBI-270623/3330
Affected Version(s): 11.0					
Access of Resource Using Incompatible Type ('Type Confusion')	05-Jun-2023	8.8	Type confusion in V8 in Google Chrome prior to 114.0.5735.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-3079**	N/A	O-DEB-DEBI-270623/3331
Missing Release of Memory	06-Jun-2023	3.3	A vulnerability was found in the pthread_create()	N/A	O-DEB-DEBI-270623/3332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
after Effective Lifetime			function in libcap. This issue may allow a malicious actor to use cause __real_pthread_create( ) to return an error, which can exhaust the process memory. **CVE ID : CVE-2023-2602**		
Affected Version(s): 12.0					
Access of Resource Using Incompatible Type ('Type Confusion')	05-Jun-2023	8.8	Type confusion in V8 in Google Chrome prior to 114.0.5735.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-3079**	N/A	O-DEB-DEBI-270623/3333
Missing Release of Memory after Effective Lifetime	06-Jun-2023	3.3	A vulnerability was found in the pthread_create() function in libcap. This issue may allow a malicious actor to use cause __real_pthread_create( ) to return an error, which can exhaust the process memory. **CVE ID : CVE-2023-2602**	N/A	O-DEB-DEBI-270623/3334
Vendor: Dell					
Product: os_recovery_tool					
Affected Version(s): 2.2.4013					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	01-Jun-2023	7.8	Dell OS Recovery Tool, versions 2.2.4013 and 2.3.7012.0, contain an Improper Access Control Vulnerability. A local authenticated non-administrator user could potentially exploit this vulnerability in order to elevate privileges on the system. **CVE ID : CVE-2023-28066**	https://www.dell.com/support/kbdoc/en-us/000212575/dsa-2023-147	O-DEL-OS_R-270623/3335
Affected Version(s): 2.3.7012.0					
Improper Access Control	01-Jun-2023	7.8	Dell OS Recovery Tool, versions 2.2.4013 and 2.3.7012.0, contain an Improper Access Control Vulnerability. A local authenticated non-administrator user could potentially exploit this vulnerability in order to elevate privileges on the system. **CVE ID : CVE-2023-28066**	https://www.dell.com/support/kbdoc/en-us/000212575/dsa-2023-147	O-DEL-OS_R-270623/3336
Vendor: Dlink					
Product: di-7500g-ci_firmware					
Affected Version(s): 19.05.29a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jun-2023	5.4	A Cross Site Scripting (XSS) vulnerability in D-Link DI-7500G-CI-19.05.29A allows attackers to execute arbitrary code via uploading a crafted HTML file to the interface /auth_pic.cgi. **CVE ID : CVE-2023-34856**	N/A	O-DLI-DI-7-270623/3337
Product: dir-842v2_firmware					
Affected Version(s): 1.0.3					
N/A	07-Jun-2023	8.8	An issue in D-Link DIR-842V2 v1.0.3 allows attackers to execute arbitrary commands via importing a crafted file. **CVE ID : CVE-2023-33781**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--270623/3338
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jun-2023	8.8	D-Link DIR-842V2 v1.0.3 was discovered to contain a command injection vulnerability via the iperf3 diagnostics function. **CVE ID : CVE-2023-33782**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--270623/3339
Vendor: Draytek					
Product: vigor1000b_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches	N/A	O-DRA-VIGO-270623/3340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website.	N/A	O-DRA-VIGO-270623/3341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33778		
Product: vigor130_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3342
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which	N/A	O-DRA-VIGO-270623/3343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor165_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3344
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points	N/A	O-DRA-VIGO-270623/3345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor166_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and	N/A	O-DRA-VIGO-270623/3346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3347
Product: vigor167_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to	N/A	O-DRA-VIGO-270623/3348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3349
Product: vigor2135ac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3350
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create	N/A	O-DRA-VIGO-270623/3351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2135ax_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3352
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware	N/A	O-DRA-VIGO-270623/3353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2135fvac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3354
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3355
Product: vigor2135vac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are	N/A	O-DRA-VIGO-270623/3356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3357
Product: vigor2620ln_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and	N/A	O-DRA-VIGO-270623/3358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3359
Product: vigor2620l_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3360
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are	N/A	O-DRA-VIGO-270623/3361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2763ac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3362
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and	N/A	O-DRA-VIGO-270623/3363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2765ac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3365
Product: vigor2765ax_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected	N/A	O-DRA-VIGO-270623/3366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3367
Product: vigor2765vac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches	N/A	O-DRA-VIGO-270623/3368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website.	N/A	O-DRA-VIGO-270623/3369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33778		
Product: vigor2766ac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3370
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which	N/A	O-DRA-VIGO-270623/3371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2766ax_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3372
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points	N/A	O-DRA-VIGO-270623/3373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2766vac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and	N/A	O-DRA-VIGO-270623/3374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3375
Product: vigor2832n_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to	N/A	O-DRA-VIGO-270623/3376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3377
Product: vigor2862ac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3378
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create	N/A	O-DRA-VIGO-270623/3379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2862bn_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3380
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware	N/A	O-DRA-VIGO-270623/3381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2862b_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3382
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3383
Product: vigor2862lac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are	N/A	O-DRA-VIGO-270623/3384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3385
Product: vigor2862ln_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and	N/A	O-DRA-VIGO-270623/3386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3387
Product: vigor2862l_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3388
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are	N/A	O-DRA-VIGO-270623/3389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2862n_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3390
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and	N/A	O-DRA-VIGO-270623/3391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2862vac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3393
Product: vigor2865ac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected	N/A	O-DRA-VIGO-270623/3394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3395
Product: vigor2865ax_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches	N/A	O-DRA-VIGO-270623/3396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website.	N/A	O-DRA-VIGO-270623/3397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33778		
Product: vigor2865lac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3398
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which	N/A	O-DRA-VIGO-270623/3399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2865l_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3400
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points	N/A	O-DRA-VIGO-270623/3401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2865vac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and	N/A	O-DRA-VIGO-270623/3402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3403
Product: vigor2866ac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to	N/A	O-DRA-VIGO-270623/3404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3405
Product: vigor2866ax_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3406
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create	N/A	O-DRA-VIGO-270623/3407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2866lac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3408
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware	N/A	O-DRA-VIGO-270623/3409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2866l_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3410
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3411
Product: vigor2866vac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are	N/A	O-DRA-VIGO-270623/3412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3413
Product: vigor2915ac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and	N/A	O-DRA-VIGO-270623/3414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3415
Product: vigor2926_plus_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3416
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are	N/A	O-DRA-VIGO-270623/3417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2927ac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3418
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and	N/A	O-DRA-VIGO-270623/3419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2927ax_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3421
Product: vigor2927f_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected	N/A	O-DRA-VIGO-270623/3422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3423
Product: vigor2927lac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches	N/A	O-DRA-VIGO-270623/3424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website.	N/A	O-DRA-VIGO-270623/3425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33778		
Product: vigor2927l_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3426
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which	N/A	O-DRA-VIGO-270623/3427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2927vac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3428
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points	N/A	O-DRA-VIGO-270623/3429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigor2962_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and	N/A	O-DRA-VIGO-270623/3430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3431
Product: vigor3910_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to	N/A	O-DRA-VIGO-270623/3432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3433
Product: vigorap_1000c_firmware					
Affected Version(s): * Up to (excluding) 1.4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3434
Product: vigorap_1060c_firmware					
Affected Version(s): * Up to (excluding) 1.4.0					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are	N/A	O-DRA-VIGO-270623/3435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorap_903_firmware					
Affected Version(s): * Up to (excluding) 1.4.0					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3436
Product: vigorap_906_firmware					
Affected Version(s): * Up to (excluding) 1.4.0					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches	N/A	O-DRA-VIGO-270623/3437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorap_912c_firmware					
Affected Version(s): * Up to (excluding) 1.4.0					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website.	N/A	O-DRA-VIGO-270623/3438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33778		
Product: vigorap_918r_firmware					
Affected Version(s): * Up to (excluding) 1.4.0					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3439
Product: vigorap_960c_firmware					
Affected Version(s): * Up to (excluding) 1.4.0					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded	N/A	O-DRA-VIGO-270623/3440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorlte_200n_firmware					
Affected Version(s): * Up to (excluding) 3.9.6					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3441
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.4					
Use of Hard-	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4,	N/A	O-DRA-VIGO-270623/3442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorswitch_fx2120_firmware					
Affected Version(s): * Up to (excluding) 2.6.7					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and	N/A	O-DRA-VIGO-270623/3443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorswitch_g1080_firmware					
Affected Version(s): * Up to (excluding) 2.6.7					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3444
Product: vigorswitch_g1085_firmware					
Affected Version(s): * Up to (excluding) 2.6.7					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware	N/A	O-DRA-VIGO-270623/3445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorswitch_g1282_firmware					
Affected Version(s): * Up to (excluding) 2.6.7					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3446
Product: vigorswitch_g2100_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.6.7					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3447
Product: vigorswitch_g2121_firmware					
Affected Version(s): * Up to (excluding) 2.6.7					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected	N/A	O-DRA-VIGO-270623/3448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorswitch_g2280x_firmware					
Affected Version(s): * Up to (excluding) 2.6.7					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3449
Product: vigorswitch_g2540xs_firmware					
Affected Version(s): * Up to (excluding) 2.6.7					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points	N/A	O-DRA-VIGO-270623/3450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorswitch_p1282_firmware					
Affected Version(s): * Up to (excluding) 2.6.7					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and	N/A	O-DRA-VIGO-270623/3451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorswitch_p2100_firmware					
Affected Version(s): * Up to (excluding) 2.6.7					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3452
Product: vigorswitch_p2280x_firmware					
Affected Version(s): * Up to (excluding) 2.6.7					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware	N/A	O-DRA-VIGO-270623/3453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorswitch_p2540xs_firmware					
Affected Version(s): * Up to (excluding) 2.6.7					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3454
Product: vigorswitch_pq2121x_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.6.7					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3455
Product: vigorswitch_pq2200xb_firmware					
Affected Version(s): * Up to (excluding) 2.6.7					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected	N/A	O-DRA-VIGO-270623/3456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Product: vigorswitch_q2121x_firmware					
Affected Version(s): * Up to (excluding) 2.6.7					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**	N/A	O-DRA-VIGO-270623/3457
Product: vigorswitch_q2200x_firmware					
Affected Version(s): * Up to (excluding) 2.6.7					
Use of Hard-coded Credentials	01-Jun-2023	9.8	Draytek Vigor Routers firmware versions below 3.9.6/4.2.4, Access Points	N/A	O-DRA-VIGO-270623/3458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions below v1.4.0, Switches firmware versions below 2.6.7, and Myvigor firmware versions below 2.3.2 were discovered to use hardcoded encryption keys which allows attackers to bind any affected device to their own account. Attackers are then able to create WCF and DrayDDNS licenses and synchronize them from the website. **CVE ID : CVE-2023-33778**		
Vendor: fanuc					
Product: roboguide_handlingpro_firmware					
Affected Version(s): * Up to (excluding) 9_rev.zd					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Jun-2023	7.5	FANUC ROBOGUIDE-HandlingPRO Versions 9 Rev.ZD and prior is vulnerable to a path traversal, which could allow an attacker to remotely read files on the system running the affected software. **CVE ID : CVE-2023-1864**	N/A	O-FAN-ROBO-270623/3459
Vendor: Fedoraproject					
Product: fedora					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 37					
Missing Release of Memory after Effective Lifetime	06-Jun-2023	3.3	A vulnerability was found in the pthread_create() function in libcap. This issue may allow a malicious actor to use cause __real_pthread_create( ) to return an error, which can exhaust the process memory. **CVE ID : CVE-2023-2602**	N/A	O-FED-FEDO-270623/3460
Affected Version(s): 38					
Access of Resource Using Incompatible Type ('Type Confusion')	05-Jun-2023	8.8	Type confusion in V8 in Google Chrome prior to 114.0.5735.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-3079**	N/A	O-FED-FEDO-270623/3461
Missing Release of Memory after Effective Lifetime	06-Jun-2023	3.3	A vulnerability was found in the pthread_create() function in libcap. This issue may allow a malicious actor to use cause __real_pthread_create( ) to return an error, which can exhaust the process memory. **CVE ID : CVE-2023-2602**	N/A	O-FED-FEDO-270623/3462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: furbo					
Product: dog_camera_firmware					
Affected Version(s): 542					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Jun-2023	8.8	Furbo dog camera has insufficient filtering for special parameter of device log management function. An unauthenticated remote attacker in the Bluetooth network with normal user privileges can exploit this vulnerability to perform command injection attack to execute arbitrary system commands or disrupt service. **CVE ID : CVE-2023-28704**	N/A	O-FUR-DOG_-270623/3463
Vendor: gallagher					
Product: controller_6000_firmware					
Affected Version(s): * Up to (excluding) 8.50.230201a					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jun-2023	9.8	Controller 6000 is vulnerable to a buffer overflow via the Controller diagnostic web interface upload feature. This issue affects Controller 6000: before vCR8.80.230201a,	https://security.gallagher.com/en-NZ/Security-Advisories/CVE-2023-24584	O-GAL-CONT-270623/3464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before vCR8.70.230201a, before vCR8.60.230201b, before vCR8.50.230201a, all versions of vCR8.40 and prior. **CVE ID : CVE-2023-24584**		
Affected Version(s): From (including) 8.60 Up to (excluding) 8.60.230201b					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jun-2023	9.8	Controller 6000 is vulnerable to a buffer overflow via the Controller diagnostic web interface upload feature. This issue affects Controller 6000: before vCR8.80.230201a, before vCR8.70.230201a, before vCR8.60.230201b, before vCR8.50.230201a, all versions of vCR8.40 and prior.	https://security.gallagher.com/en-NZ/Security-Advisories/CVE-2023-24584	O-GAL-CONT-270623/3465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24584		
Affected Version(s): From (including) 8.70 Up to (excluding) 8.70.230201a					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jun-2023	9.8	Controller 6000 is vulnerable to a buffer overflow via the Controller diagnostic web interface upload feature. This issue affects Controller 6000: before vCR8.80.230201a, before vCR8.70.230201a, before vCR8.60.230201b, before vCR8.50.230201a, all versions of vCR8.40 and prior. **CVE ID : CVE-2023-24584**	https://security.gallagher.com/en-NZ/Security-Advisories/CVE-2023-24584	O-GAL-CONT-270623/3466
Affected Version(s): From (including) 8.80 Up to (excluding) 8.80.230201a					
Buffer Copy without Checking Size of Input ('Classic	01-Jun-2023	9.8	Controller 6000 is vulnerable to a buffer overflow via the Controller diagnostic web interface upload feature.	https://security.gallagher.com/en-NZ/Security-Advisories/CVE-2023-24584	O-GAL-CONT-270623/3467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			This issue affects Controller 6000: before vCR8.80.230201a, before vCR8.70.230201a, before vCR8.60.230201b, before vCR8.50.230201a, all versions of vCR8.40 and prior. **CVE ID : CVE-2023-24584**		
Vendor: Google					
Product: android					
Affected Version(s): 10.0					
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges. **CVE ID : CVE-2023-30863**	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624998	O-GOO-ANDR-270623/3468
Missing Authorization	06-Jun-2023	7.8	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624998	O-GOO-ANDR-270623/3469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges. **CVE ID : CVE-2023-30864**		
Missing Authorization	06-Jun-2023	5.5	In dialer service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30865**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624798	O-GOO-ANDR-270623/3470
Missing Authorization	06-Jun-2023	5.5	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30866**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624798	O-GOO-ANDR-270623/3471
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30914**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624798	O-GOO-ANDR-270623/3472
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624798	O-GOO-ANDR-270623/3473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. **CVE ID : CVE-2023-30915**		
Affected Version(s): 11.0					
Out-of-bounds Read	06-Jun-2023	6.7	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07843845; Issue ID: ALPS07843845. **CVE ID : CVE-2023-20723**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3474
Out-of-bounds Read	06-Jun-2023	6.7	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07843845; Issue ID: ALPS07843841. **CVE ID : CVE-2023-20724**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3475
Missing Authorization	06-Jun-2023	5.5	In dialer service, there is a missing permission check. This could lead to local information disclosure with no	https://www.unisoc.com/en_us/secy/announcementDetail/166482	O-GOO-ANDR-270623/3476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. **CVE ID : CVE-2023-30865**	23614147624 98	
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30914**	https://www.unisoc.com/en_us/secy/announcementDetail/166482 23614147624 98	O-GOO-ANDR-270623/3477
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30915**	https://www.unisoc.com/en_us/secy/announcementDetail/166482 23614147624 98	O-GOO-ANDR-270623/3478
Affected Version(s): 12.0					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3480
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3481
Out-of-bounds Read	06-Jun-2023	6.7	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07843845; Issue ID: ALPS07843845. **CVE ID : CVE-2023-20723**		
Out-of-bounds Read	06-Jun-2023	6.7	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07843845; Issue ID: ALPS07843841. **CVE ID : CVE-2023-20724**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3483
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3485
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3486
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3488
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3489
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a 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/June-2023	O-GOO-ANDR-270623/3490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**		
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3491
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559840. **CVE ID : CVE-2023-20740**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3492
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation	https://corp.mediatek.com/product-security-	O-GOO-ANDR-270623/3493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519142. **CVE ID : CVE-2023-20743**	bulletin/June-2023	
Use After Free	06-Jun-2023	6.7	In vcu, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519200. **CVE ID : CVE-2023-20744**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3494
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07560694. **CVE ID : CVE-2023-20745**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3495
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds	https://corp.mediatek.com	O-GOO-ANDR-270623/3496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	/product-security-bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07825502; Issue ID: ALPS07825502. **CVE ID : CVE-2023-20751**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3497
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07826586; Issue ID: ALPS07826586. **CVE ID : CVE-2023-20752**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3499
Missing Authorization	06-Jun-2023	5.5	In dialer service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30865**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	O-GOO-ANDR-270623/3500
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30914**	https://www.unisoc.com/en_us/secy/announcementDetail/1664823614147624998	O-GOO-ANDR-270623/3501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Jun-2023	5.5	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30915**	https://www.unisoc.com/en_us/secy/announcementDetail/16648223614147624998	O-GOO-ANDR-270623/3502
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3503
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3505
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3506
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**		
Access of Resource Using Incompatible Type ('Type Confusion')	06-Jun-2023	4.4	In vcu, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3508
Affected Version(s): 13.0					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3509
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**		
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3511
Out-of-bounds Read	06-Jun-2023	6.7	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07843845; Issue ID: ALPS07843845. **CVE ID : CVE-2023-20723**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3512
Out-of-bounds Read	06-Jun-2023	6.7	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This	https://corp.mediatek.com/product-security-	O-GOO-ANDR-270623/3513

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: ALPS07843845; Issue ID: ALPS07843841. **CVE ID : CVE-2023-20724**	bulletin/June-2023	
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3514
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS07573480; Issue ID: ALPS07573480. **CVE ID : CVE-2023-20732**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645149. **CVE ID : CVE-2023-20733**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3516
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645184. **CVE ID : CVE-2023-20734**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3517
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645178. **CVE ID : CVE-2023-20735**		
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645167. **CVE ID : CVE-2023-20737**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3519
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645173. **CVE ID : CVE-2023-20738**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3520
Out-of-bounds Write	06-Jun-2023	6.7	In vcu, there is a possible memory corruption due to a	https://corp.mediatek.com/product-	O-GOO-ANDR-270623/3521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559819; Issue ID: ALPS07559819. **CVE ID : CVE-2023-20739**	security-bulletin/June-2023	
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519142. **CVE ID : CVE-2023-20743**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3522
Use After Free	06-Jun-2023	6.7	In vcu, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519200. **CVE ID : CVE-2023-20744**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07560694. **CVE ID : CVE-2023-20745**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3524
Improper Locking	06-Jun-2023	6.7	In vcu, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519142; Issue ID: ALPS07519217. **CVE ID : CVE-2023-20746**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3525
Out-of-bounds Write	06-Jun-2023	6.7	In swpm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07780926; Issue ID: ALPS07780926. **CVE ID : CVE-2023-20749**		
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07825502; Issue ID: ALPS07825502. **CVE ID : CVE-2023-20751**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3527
Out-of-bounds Write	06-Jun-2023	6.7	In keymange, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826586; Issue ID: ALPS07826586. **CVE ID : CVE-2023-20752**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3528
Concurrent Execution using Shared Resource with	06-Jun-2023	6.4	In vcu, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645149; Issue ID: ALPS07645189. **CVE ID : CVE-2023-20736**		
Missing Authorization	06-Jun-2023	5.5	In dialer service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. **CVE ID : CVE-2023-30865**	https://www.unisoc.com/en_us/secy/announcementDetail/1664822361414762498	O-GOO-ANDR-270623/3530
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588531; Issue ID: ALPS07588531. **CVE ID : CVE-2023-20727**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3531
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07573603; Issue ID: ALPS07573603. **CVE ID : CVE-2023-20728**		
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573575. **CVE ID : CVE-2023-20729**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3533
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573552; Issue ID: ALPS07573552. **CVE ID : CVE-2023-20730**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3534
Out-of-bounds Read	06-Jun-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-	O-GOO-ANDR-270623/3535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07573495; Issue ID: ALPS07573495. **CVE ID : CVE-2023-20731**	bulletin/June-2023	
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628606. **CVE ID : CVE-2023-20741**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3536
Out-of-bounds Read	06-Jun-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628591; Issue ID: ALPS07628540. **CVE ID : CVE-2023-20742**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3537
Access of Resource	06-Jun-2023	4.4	In vcu, there is a possible memory	https://corp.mediatek.com	O-GOO-ANDR-270623/3538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Using Incompatible Type ('Type Confusion')			corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519121. **CVE ID : CVE-2023-20747**	/product-security-bulletin/June-2023	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Jun-2023	4.1	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928. **CVE ID : CVE-2023-20750**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-GOO-ANDR-270623/3539
Vendor: harmonicinc					
Product: nsg_9000-6g_firmware					
Affected Version(s): -					
Missing Authorization	06-Jun-2023	6.5	In Harmonic NSG 9000-6G devices, an authenticated remote user can obtain source code by directly requesting a special path. **CVE ID : CVE-2023-33477**	N/A	O-HAR-NSG_-270623/3540
Vendor: hitrontech					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: coda-5310_firmware					
Affected Version(s): 7.2.4.7.1b3					
Improper Authentication	02-Jun-2023	9.8	Hitron Technologies CODA-5310 Telnet function with the default account and password, and there is no warning or prompt to ask users to change the default password and account. An unauthenticated remote attackers can exploit this vulnerability to obtain the administrator's privilege, resulting in performing arbitrary system operation or disrupt service. **CVE ID : CVE-2023-30603**	N/A	O-HIT-CODA-270623/3541
Missing Authentication for Critical Function	02-Jun-2023	9.8	It is identified a vulnerability of insufficient authentication in the system configuration interface of Hitron Technologies CODA-5310. An unauthorized remote attacker can exploit this vulnerability to access system configuration interface, resulting in performing arbitrary system operation or disrupt service. **CVE ID : CVE-2023-30604**	N/A	O-HIT-CODA-270623/3542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Encryption of Sensitive Data	02-Jun-2023	7.5	Hitron Technologies CODA-5310's Telnet function transfers sensitive data in plaintext. An unauthenticated remote attacker can exploit this vulnerability to access credentials of normal users and administrator. **CVE ID : CVE-2023-30602**	N/A	O-HIT-CODA-270623/3543
Vendor: HP					
Product: hp-ux					
Affected Version(s): -					
N/A	07-Jun-2023	6.5	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 could allow a privileged user to obtain highly sensitive information by enabling debug mode. IBM X-Force ID: 257104. **CVE ID : CVE-2023-33848**	https://www.ibm.com/support/pages/node/7001683, https://exchange.xforce.ibmcloud.com/vulnerabilities/257104, https://www.ibm.com/support/pages/node/7001681, https://www.ibm.com/support/pages/node/7001647	O-HP-HP-U-270623/3544
Missing Encryption of Sensitive Data	07-Jun-2023	3.7	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 could transmit sensitive information in query parameters	https://www.ibm.com/support/pages/node/7001695, https://exchange.xforce.ibmcloud.com/vulnerabilities/	O-HP-HP-U-270623/3545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could be intercepted using man in the middle techniques. IBM X-Force ID: 257105. **CVE ID : CVE-2023-33849**	257105, https://www.ibm.com/support/pages/node/7001697, https://www.ibm.com/support/pages/node/7001687	
Vendor: IBM					
Product: aix					
Affected Version(s): -					
N/A	07-Jun-2023	6.5	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 could allow a privileged user to obtain highly sensitive information by enabling debug mode. IBM X-Force ID: 257104. **CVE ID : CVE-2023-33848**	https://www.ibm.com/support/pages/node/7001683, https://exchange.xforce.ibmcloud.com/vulnerabilities/257104, https://www.ibm.com/support/pages/node/7001681, https://www.ibm.com/support/pages/node/7001647	O-IBM-AIX-270623/3546
Missing Encryption of Sensitive Data	07-Jun-2023	3.7	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 could transmit sensitive information in query parameters that could be intercepted using man in the middle techniques. IBM X-Force ID: 257105.	https://www.ibm.com/support/pages/node/7001695, https://exchange.xforce.ibmcloud.com/vulnerabilities/257105, https://www.ibm.com/support/pages/node/7001697,	O-IBM-AIX-270623/3547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33849	https://www.ibm.com/support/pages/node/7001687	
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
N/A	08-Jun-2023	9.6	IBM Sterling Partner Engagement Manager 6.1, 6.2, and 6.2.1 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 245891. **CVE ID : CVE-2023-23482**	https://exchange.xforce.ibmcloud.com/vulnerabilities/245891, https://www.ibm.com/support/pages/node/7001569	O-LIN-LINU-270623/3548
Insufficient Session Expiration	05-Jun-2023	8.8	IBM Security Guardium 11.5 could allow a user to take over another user's session due to insufficient session expiration. IBM X-Force ID: 243657. **CVE ID : CVE-2023-0041**	https://www.ibm.com/support/pages/node/7000021, https://exchange.xforce.ibmcloud.com/vulnerabilities/243657	O-LIN-LINU-270623/3549
N/A	07-Jun-2023	6.5	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS	https://www.ibm.com/support/pages/node/7001683,	O-LIN-LINU-270623/3550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TX Advanced 10.1, and 11.1 could allow a privileged user to obtain highly sensitive information by enabling debug mode. IBM X-Force ID: 257104. **CVE ID : CVE-2023-33848**	https://exchange.xforce.ibmcloud.com/vulnerabilities/257104, https://www.ibm.com/support/pages/node/7001681, https://www.ibm.com/support/pages/node/7001647	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jun-2023	5.4	IBM Sterling Partner Engagement Manager 6.1, 6.2, and 6.2.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 245885. **CVE ID : CVE-2023-23480**	https://www.ibm.com/support/pages/node/7001563, https://exchange.xforce.ibmcloud.com/vulnerabilities/245885	O-LIN-LINU-270623/3551
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jun-2023	5.4	IBM Sterling Partner Engagement Manager 6.1, 6.2, and 6.2.1 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to	https://www.ibm.com/support/pages/node/7001561, https://exchange.xforce.ibmcloud.com/vulnerabilities/245889	O-LIN-LINU-270623/3552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credentials disclosure within a trusted session. IBM X-Force ID: 245889. **CVE ID : CVE-2023-23481**		
Missing Encryption of Sensitive Data	07-Jun-2023	3.7	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 could transmit sensitive information in query parameters that could be intercepted using man in the middle techniques. IBM X-Force ID: 257105. **CVE ID : CVE-2023-33849**	https://www.ibm.com/support/pages/node/7001695, https://exchange.xforce.ibmcloud.com/vulnerabilities/257105, https://www.ibm.com/support/pages/node/7001697, https://www.ibm.com/support/pages/node/7001687	O-LIN-LINU-270623/3553
Affected Version(s): * Up to (excluding) 6.0					
Use After Free	05-Jun-2023	7.8	A use after free vulnerability was found in prepare_to_relocate in fs/btrfs/relocation.c in btrfs in the Linux Kernel. This possible flaw can be triggered by calling btrfs_ioctl_balance() before calling btrfs_ioctl_defrag(). **CVE ID : CVE-2023-3111**	https://patchwork.kernel.org/project/linux-btrfs/patch/202207210748 29.2905233-1-r33s3n6@gmail.com/	O-LIN-LINU-270623/3554
Affected Version(s): * Up to (excluding) 6.3					
Use After Free	01-Jun-2023	5.5	A use after free flaw was found in hfsplus_put_super in	https://git.kernel.org/pub/scm/linux/ke	O-LIN-LINU-270623/3555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fs/hfsplus/super.c in the Linux Kernel. This flaw could allow a local user to cause a denial of service problem. **CVE ID : CVE-2023-2985**	rnel/git/torvalds/linux.git/commit/?id=07db5e247ab5858439b14dd7cc1fe538b9efcf32	
Affected Version(s): 4.19					
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796914; Issue ID: ALPS07796914. **CVE ID : CVE-2023-20712**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-LIN-LINU-270623/3556
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796900; Issue ID: ALPS07796900. **CVE ID : CVE-2023-20715**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-LIN-LINU-270623/3557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07796883; Issue ID: ALPS07796883. **CVE ID : CVE-2023-20716**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-LIN-LINU-270623/3558
Affected Version(s): 6.0					
Use After Free	05-Jun-2023	7.8	A use after free vulnerability was found in prepare_to_relocate in fs/btrfs/relocation.c in btrfs in the Linux Kernel. This possible flaw can be triggered by calling btrfs_ioctl_balance() before calling btrfs_ioctl_defrag(). **CVE ID : CVE-2023-3111**	https://patchwork.kernel.org/project/linux-btrfs/patch/202207210748 29.2905233-1-r33s3n6@gmail.com/	O-LIN-LINU-270623/3559
Affected Version(s): From (including) 6.3 Up to (including) 6.3.6					
Out-of-bounds Write	01-Jun-2023	7.8	A flaw was found in the fixed buffer registration code for io_uring (io_sqe_buffer_register in io_uring/rsrc.c) in the Linux kernel that allows out-of-bounds access to physical memory beyond the end of the buffer. This	N/A	O-LIN-LINU-270623/3560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			flaw enables full local privilege escalation. **CVE ID : CVE-2023-2598**		
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
N/A	02-Jun-2023	8.1	After downloading a Windows <code>.url</code> shortcut from the local filesystem, an attacker could supply a remote path that would lead to unexpected network requests from the operating system. This also had the potential to leak NTLM credentials to the resource. *This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25734**	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/advisories/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/, https://bugzilla.mozilla.org/show_bug.cgi?id=1784451	O-MIC-WIND-270623/3561
Out-of-bounds Read	02-Jun-2023	6.5	Members of the <code>DEVMODEW</code> struct set by the printer device driver weren't being validated and could have resulted in invalid values which	https://www.mozilla.org/security/advisories/mfsa2023-05/, https://www.mozilla.org/security/adviso	O-MIC-WIND-270623/3562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in turn would cause the browser to attempt out of bounds access to related variables. *This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8. **CVE ID : CVE-2023-25738**	ries/mfsa2023-07/, https://www.mozilla.org/security/advisories/mfsa2023-06/	
Out-of-bounds Write	05-Jun-2023	5.5	A buffer overflow in EasyPlayerPro-Win v3.2.19.0106 to v3.6.19.0823 allows attackers to cause a Denial of Service (DoS) via a crafted XML file. **CVE ID : CVE-2023-33693**	https://github.com/tsingsee/EasyPlayerPro-Win/pull/24	O-MIC-WIND-270623/3563
Vendor: mitrastar					
Product: gpt-2741gnac_firmware					
Affected Version(s): ar_g5.8_110wvn0b7_2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jun-2023	7.2	A command injection vulnerability was found in the ping functionality of the MitraStar GPT-2741GNAC router (firmware version AR_g5.8_110WVN0b7_2). The vulnerability allows an authenticated user to execute arbitrary OS	N/A	O-MIT-GPT--270623/3564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands by sending specially crafted input to the router via the ping function. **CVE ID : CVE-2023-33381**		
Vendor: Netgear					
Product: d6220_firmware					
Affected Version(s): 1.0.0.80					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jun-2023	8.8	Netgear D6220 with Firmware Version 1.0.0.80, D8500 with Firmware Version 1.0.3.60, R6700 with Firmware Version 1.0.2.26, and R6900 with Firmware Version 1.0.2.26 are vulnerable to Command Injection. If an attacker gains web management privileges, they can inject commands into the post request parameters, gaining shell privileges. **CVE ID : CVE-2023-33533**	https://www.netgear.com/about/security/	O-NET-D622-270623/3565
Product: d8500_firmware					
Affected Version(s): 1.0.3.60					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jun-2023	8.8	Netgear D6220 with Firmware Version 1.0.0.80, D8500 with Firmware Version 1.0.3.60, R6700 with Firmware Version 1.0.2.26, and R6900 with Firmware Version 1.0.2.26 are vulnerable to	https://www.netgear.com/about/security/	O-NET-D850-270623/3566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Command Injection. If an attacker gains web management privileges, they can inject commands into the post request parameters, gaining shell privileges. **CVE ID : CVE-2023-33533**		
Product: r6250_firmware					
Affected Version(s): 1.0.4.48					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jun-2023	9.8	There is a command injection vulnerability in the Netgear R6250 router with Firmware Version 1.0.4.48. If an attacker gains web management privileges, they can inject commands into the post request parameters, thereby gaining shell privileges. **CVE ID : CVE-2023-33532**	N/A	O-NET-R625-270623/3567
Product: r6700_firmware					
Affected Version(s): 1.0.2.26					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jun-2023	8.8	Netgear D6220 with Firmware Version 1.0.0.80, D8500 with Firmware Version 1.0.3.60, R6700 with Firmware Version 1.0.2.26, and R6900 with Firmware Version 1.0.2.26 are vulnerable to Command Injection. If an attacker gains web	https://www.netgear.com/about/security/	O-NET-R670-270623/3568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management privileges, they can inject commands into the post request parameters, gaining shell privileges. **CVE ID : CVE-2023-33533**		
Product: r6900_firmware					
Affected Version(s): 1.0.2.26					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jun-2023	8.8	Netgear D6220 with Firmware Version 1.0.0.80, D8500 with Firmware Version 1.0.3.60, R6700 with Firmware Version 1.0.2.26, and R6900 with Firmware Version 1.0.2.26 are vulnerable to Command Injection. If an attacker gains web management privileges, they can inject commands into the post request parameters, gaining shell privileges. **CVE ID : CVE-2023-33533**	https://www.netgear.com/about/security/	O-NET-R690-270623/3569
Vendor: openwrt					
Product: openwrt					
Affected Version(s): 19.07.0					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a 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/June-2023	O-OPE-OPEN-270623/3570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**		
Affected Version(s): 21.02.0					
Out-of-bounds Write	06-Jun-2023	6.7	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only); Issue ID: ALPS07734004 / ALPS07874358 (For MT6880, MT6890, MT6980, MT6990 only). **CVE ID : CVE-2023-20725**	https://corp.mediatek.com/product-security-bulletin/June-2023	O-OPE-OPEN-270623/3571
Vendor: planet					
Product: wdrt-1800ax_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.01-cp21					
Improper Authentication	07-Jun-2023	9.8	An issue in Planet Technologies WDRT-1800AX v1.01-CP21 allows attackers to bypass authentication and escalate privileges to root via manipulation of the LoginStatus cookie. **CVE ID : CVE-2023-33553**	N/A	O-PLA-WDRT-270623/3572
Vendor: Qualcomm					
Product: 205_mobile_platform_firmware					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-205_-270623/3573
Product: 315_5g_iot_modem_firmware					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-315_-270623/3574
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-315_-270623/3575
Product: apq8017_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-APQ8-270623/3576
Product: apq8064au_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-APQ8-270623/3577
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-APQ8-270623/3578
Product: apq8076_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-APQ8-270623/3579
Product: apq8092_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF	https://www.qualcomm.com/company/product-	O-QUA-APQ8-270623/3580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	security/bulletins/june-2023-bulletin	
Product: apq8094_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-APQ8-270623/3581
Product: aqt1000_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-AQT1-270623/3582
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-AQT1-270623/3583
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-AQT1-270623/3584
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending	https://www.qualcomm.com/company/	O-QUA-AQT1-270623/3585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	product-security/bulletins/june-2023-bulletin	
Product: ar8031_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-AR80-270623/3586
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-AR80-270623/3587
Product: ar8035_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-AR80-270623/3588
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-AR80-270623/3589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-AR80-270623/3590
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-AR80-270623/3591
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-AR80-270623/3592
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-AR80-270623/3593
Product: ar9380_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-AR93-270623/3594
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/	O-QUA-AR93-270623/3595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	product-security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-AR93-270623/3596
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-AR93-270623/3597
Product: c-v2x9150_firmware					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-C-V2-270623/3598
Product: csr8811_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-CSR8-270623/3599
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/product-	O-QUA-CSR8-270623/3600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-CSR8-270623/3601
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-CSR8-270623/3602
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-CSR8-270623/3603
Product: csra6620_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-CSRA-270623/3604
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulle	O-QUA-CSRA-270623/3605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-CSRA-270623/3606
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-CSRA-270623/3607
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-CSRA-270623/3608
Product: csra6640_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-CSRA-270623/3609
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-CSRA-270623/3610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-CSRA-270623/3611
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-CSRA-270623/3612
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-CSRA-270623/3613
Product: csrb31024_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-CSRB-270623/3614
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-CSRB-270623/3615
Product: flight_rb5_5g_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-FLIG-270623/3616
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-FLIG-270623/3617
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-FLIG-270623/3618
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-FLIG-270623/3619
Product: home_hub_100_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-HOME-270623/3620
Product: immersive_home_214_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3621
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3622
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3623
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3624
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3625
Product: immersive_home_216_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF	https://www.qualcomm.com/company/product-	O-QUA-IMME-270623/3626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3627
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3628
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3629
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3630
Product: immersive_home_316_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-IMME-270623/3631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3632
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3633
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3634
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3635
Product: immersive_home_318_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3637
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3638
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3639
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IMME-270623/3640
Product: ipq4018_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ4-270623/3641
Product: ipq4019_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ4-270623/3642
Product: ipq4028_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ4-270623/3643
Product: ipq4029_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ4-270623/3644
Product: ipq5010_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ5-270623/3645
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-IPQ5-270623/3646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21658	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ5-270623/3647
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ5-270623/3648
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ5-270623/3649
Product: ipq5028_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ5-270623/3650
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ5-270623/3651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ5-270623/3652
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ5-270623/3653
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ5-270623/3654
Product: ipq6000_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3655
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3656
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	O-QUA-IPQ6-270623/3657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3658
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3659
Product: ipq6005_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3660
Product: ipq6010_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3661
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/product-	O-QUA-IPQ6-270623/3662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3663
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3664
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3665
Product: ipq6018_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3666
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-IPQ6-270623/3667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21658	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3668
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3669
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3670
Product: ipq6028_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3671
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3673
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3674
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ6-270623/3675
Product: ipq8064_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3676
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3677
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-270623/3678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3679
Product: ipq8065_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3680
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3681
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3682
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulle	O-QUA-IPQ8-270623/3683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Product: ipq8068_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3684
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3685
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3686
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3687
Product: ipq8069_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-IPQ8-270623/3688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Product: ipq8070a_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3689
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3690
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3691
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3692
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3693
Product: ipq8070_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3694
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3695
Product: ipq8071a_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3696
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3697
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3699
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3700
Product: ipq8071_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3701
Product: ipq8072a_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3702
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3704
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3705
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3706
Product: ipq8072_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3707
Product: ipq8074a_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3709
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3710
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3711
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3712
Product: ipq8074_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3713
Product: ipq8076a_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3714
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3715
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3716
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3717
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3718
Product: ipq8076_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-270623/3719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3720
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3721
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3722
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3723
Product: ipq8078a_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-IPQ8-270623/3724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3725
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3726
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3727
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3728
Product: ipq8078_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3730
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3731
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3732
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3733
Product: ipq8173_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3734
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-270623/3735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3736
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3737
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3738
Product: ipq8174_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3739
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-IPQ8-270623/3740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21658	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3741
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3742
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ8-270623/3743
Product: ipq9008_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ9-270623/3744
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ9-270623/3745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ9-270623/3746
Product: ipq9574_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ9-270623/3747
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ9-270623/3748
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ9-270623/3749
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-IPQ9-270623/3750
Product: mdm8215_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-MDM8-270623/3751
Product: mdm9215_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-MDM9-270623/3752
Product: mdm9250_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-MDM9-270623/3753
Product: mdm9310_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-MDM9-270623/3754
Product: mdm9615_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-MDM9-270623/3755
Product: mdm9628_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-MDM9-270623/3756
Product: mdm9640_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-MDM9-270623/3757
Product: mdm9645_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-MDM9-270623/3758
Product: mdm9650_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-MDM9-270623/3759
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-MDM9-270623/3760
Product: msm8996au_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-MSM8-270623/3761
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-MSM8-270623/3762
Product: pmp8074_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-PMP8-270623/3763
Product: qam8255p_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3764
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3765
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3766
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3767
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3768
Product: qam8295p_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3769
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3770
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3771
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3772
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3773
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QAM8-270623/3774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Product: qam8650p_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3775
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3776
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3777
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3778
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3779
Product: qam8775p_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3780
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3781
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3782
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3783
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QAM8-270623/3784
Product: qca0000_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA0-270623/3785
Product: qca1023_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA1-270623/3786
Product: qca1062_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA1-270623/3787
Product: qca1064_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA1-270623/3788
Product: qca1990_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA1-270623/3789
Product: qca2062_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA2-270623/3790
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA2-270623/3791
Product: qca2064_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA2-270623/3792
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA2-270623/3793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca2065_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA2-270623/3794
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA2-270623/3795
Product: qca2066_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA2-270623/3796
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA2-270623/3797
Product: qca4010_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA4-270623/3798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Product: qca4024_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA4-270623/3799
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA4-270623/3800
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA4-270623/3801
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA4-270623/3802
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA4-270623/3803
Product: qca4531_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA4-270623/3804
Product: qca6174a_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3805
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3806
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3807
Product: qca6174_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628		
Product: qca6175a_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3809
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3810
Product: qca6310_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3811
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3812
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA6-270623/3813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3814
Product: qca6320_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3815
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3816
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3817
Product: qca6335_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA6-270623/3818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3819
Product: qca6390_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3820
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3821
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3822
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3824
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3825
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3826
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3827
Product: qca6391_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3829
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3830
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3831
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3832
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3833
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA6-270623/3834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3835
Product: qca6420_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3836
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3837
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3838
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address.	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21669		
Product: qca6421_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3840
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3841
Product: qca6426_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3842
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3843
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA6-270623/3844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3845
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3846
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3847
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3848
Product: qca6428_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca6430_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3850
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3851
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3852
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3853
Product: qca6431_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659		
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3855
Product: qca6436_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3856
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3857
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3858
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3860
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3861
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3862
Product: qca6438_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3863
Product: qca6554a_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3865
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3866
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3867
Product: qca6564au_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3868
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3869
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while	https://www.qualcomm.com/company/product-	O-QUA-QCA6-270623/3870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3871
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3872
Product: qca6564a_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3873
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3874
Product: qca6564_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF	https://www.qualcomm.com/company/product-	O-QUA-QCA6-270623/3875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	security/bulletins/june-2023-bulletin	
Product: qca6574au_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3876
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3877
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3878
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3879
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670		
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3881
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3882
Product: qca6574a_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3883
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3884
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3886
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3887
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3888
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3889
Product: qca6574_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3890
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while	https://www.qualcomm.com/company/	O-QUA-QCA6-270623/3891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	product-security/bulletins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3892
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3893
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3894
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3895
Product: qca6584au_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA6-270623/3896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3897
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3898
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3899
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3900
Product: qca6584_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3901
Product: qca6595au_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3902
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3903
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3904
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3905
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3906
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA6-270623/3907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21658	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3908
Product: qca6595_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3909
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3910
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3911
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3913
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3914
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3915
Product: qca6678aq_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3916
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3917
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/	O-QUA-QCA6-270623/3918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	product-security/bulletins/june-2023-bulletin	
Product: qca6696_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3919
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3920
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3921
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3922
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670		
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3924
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3925
Product: qca6698aq_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3926
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3927
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3929
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3930
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3931
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3932
Product: qca6797aq_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3933
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP	https://www.qualcomm.com/company/product-	O-QUA-QCA6-270623/3934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sends input during record use case. **CVE ID : CVE-2023-21657**	security/bulletins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3935
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3936
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA6-270623/3937
Product: qca7500_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA7-270623/3938
Product: qca8072_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/	O-QUA-QCA8-270623/3939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	product-security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3940
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3941
Product: qca8075_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3942
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3943
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA8-270623/3944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3945
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3946
Product: qca8081_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3947
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3948
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3950
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3951
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3952
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3953
Product: qca8082_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3954
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	O-QUA-QCA8-270623/3955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3956
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3957
Product: qca8084_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3958
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3959
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA8-270623/3960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3961
Product: qca8085_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3962
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3963
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3964
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3965
Product: qca8337_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3966
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3967
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3968
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3969
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3970
Product: qca8386_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3971
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3972
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3973
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA8-270623/3974
Product: qca9367_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3975
Product: qca9377_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3976
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3977
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3978
Product: qca9379_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3979
Product: qca9531_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca9558_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3981
Product: qca9561_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3982
Product: qca9880_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3983
Product: qca9882_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3984
Product: qca9886_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3985
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3986
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3987
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3988
Product: qca9887_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3989
Product: qca9888_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3990
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3991
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3992
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3993
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3994
Product: qca9889_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF	https://www.qualcomm.com/company/product-	O-QUA-QCA9-270623/3995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3996
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3997
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3998
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/3999
Product: qca9898_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA9-270623/4000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Product: qca9980_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4001
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4002
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4003
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4004
Product: qca9982_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA9-270623/4005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Product: qca9984_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4006
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4007
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4008
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4009
Product: qca9985_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA9-270623/4010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4011
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4012
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4013
Product: qca9986_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4014
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4016
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4017
Product: qca9990_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4018
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4019
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4020
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon	https://www.qualcomm.com/company/	O-QUA-QCA9-270623/4021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or probe-response frame. **CVE ID : CVE-2023-21661**	product-security/bulletins/june-2023-bulletin	
Product: qca9992_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4022
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4023
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4024
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4025
Product: qca9994_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF	https://www.qualcomm.com/company/product-	O-QUA-QCA9-270623/4026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4027
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4028
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCA9-270623/4029
Product: qcc2073_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCC2-270623/4030
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCC2-270623/4031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21658	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCC2-270623/4032
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCC2-270623/4033
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCC2-270623/4034
Product: qcc2076_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCC2-270623/4035
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCC2-270623/4036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCC2-270623/4037
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCC2-270623/4038
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCC2-270623/4039
Product: qcm2290_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM2-270623/4040
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM2-270623/4041
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command	https://www.qualcomm.com/company/product-	O-QUA-QCM2-270623/4042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM2-270623/4043
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM2-270623/4044
Product: qcm4290_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM4-270623/4045
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM4-270623/4046
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCM4-270623/4047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM4-270623/4048
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM4-270623/4049
Product: qcm4325_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM4-270623/4050
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM4-270623/4051
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM4-270623/4052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM4-270623/4053
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM4-270623/4054
Product: qcm4490_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM4-270623/4055
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM4-270623/4056
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM4-270623/4057
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/	O-QUA-QCM4-270623/4058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	product-security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM4-270623/4059
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM4-270623/4060
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM4-270623/4061
Product: qcm6125_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM6-270623/4062
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCM6-270623/4063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Product: qcm6490_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM6-270623/4064
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM6-270623/4065
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM6-270623/4066
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM6-270623/4067
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM6-270623/4068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCM6-270623/4069
Product: qcn5021_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4070
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4071
Product: qcn5022_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4072
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4074
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4075
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4076
Product: qcn5024_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4077
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4078
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	O-QUA-QCN5-270623/4079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4080
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4081
Product: qcn5052_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4082
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4083
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCN5-270623/4084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4085
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4086
Product: qcn5054_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4087
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4088
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4090
Product: qcn5064_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4091
Product: qcn5121_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4092
Product: qcn5122_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4093
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCN5-270623/4094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21658	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4095
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4096
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4097
Product: qcn5124_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4098
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4100
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4101
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4102
Product: qcn5152_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4103
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4104
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	O-QUA-QCN5-270623/4105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4106
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4107
Product: qcn5154_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4108
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4109
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCN5-270623/4110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4111
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4112
Product: qcn5164_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4113
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4114
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4116
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4117
Product: qcn5550_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN5-270623/4118
Product: qcn6023_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4119
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4121
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4122
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4123
Product: qcn6024_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4124
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4125
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command	https://www.qualcomm.com/company/product-	O-QUA-QCN6-270623/4126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4127
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4128
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4129
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4130
Product: qcn6100_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCN6-270623/4131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21658	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4132
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4133
Product: qcn6102_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4134
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4135
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4136
Product: qcn6112_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4137
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4138
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4139
Product: qcn6122_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4140
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4142
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4143
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4144
Product: qcn6132_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4145
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4146
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	O-QUA-QCN6-270623/4147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4148
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN6-270623/4149
Product: qcn7605_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN7-270623/4150
Product: qcn7606_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN7-270623/4151
Product: qcn9000_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4152
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4153
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4154
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4155
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4156
Product: qcn9001_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/product-	O-QUA-QCN9-270623/4157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4158
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4159
Product: qcn9002_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4160
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4161
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCN9-270623/4162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Product: qcn9003_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4163
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4164
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4165
Product: qcn9011_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4166
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCN9-270623/4167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4168
Product: qcn9012_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4169
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4170
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4171
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4172
Product: qcn9022_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4173
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4174
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4175
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4176
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4177
Product: qcn9024_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4178
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4179
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4180
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4181
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4182
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCN9-270623/4183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21660	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4184
Product: qcn9070_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4185
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4186
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4187
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4189
Product: qcn9072_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4190
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4191
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4192
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4193
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon	https://www.qualcomm.com/company/product-	O-QUA-QCN9-270623/4194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or probe-response frame. **CVE ID : CVE-2023-21661**	security/bulletins/june-2023-bulletin	
Product: qcn9074_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4195
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4196
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4197
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4198
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCN9-270623/4199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21660	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4200
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4201
Product: qcn9100_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4202
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4203
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4205
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4206
Product: qcn9274_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4207
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4208
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCN9-270623/4209
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame.	https://www.qualcomm.com/company/product-	O-QUA-QCN9-270623/4210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21661	security/bulletins/june-2023-bulletin	
Product: qcs2290_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS2-270623/4211
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS2-270623/4212
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS2-270623/4213
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS2-270623/4214
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address.	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS2-270623/4215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21669		
Product: qcs400_firmware					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS4-270623/4216
Product: qcs410_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS4-270623/4217
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS4-270623/4218
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS4-270623/4219
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCS4-270623/4220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS4-270623/4221
Product: qcs4290_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS4-270623/4222
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS4-270623/4223
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS4-270623/4224
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS4-270623/4225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS4-270623/4226
Product: qcs4490_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS4-270623/4227
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS4-270623/4228
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS4-270623/4229
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS4-270623/4230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS4-270623/4231
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS4-270623/4232
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS4-270623/4233
Product: qcs605_firmware					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS6-270623/4234
Product: qcs610_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS6-270623/4235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS6-270623/4236
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS6-270623/4237
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS6-270623/4238
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS6-270623/4239
Product: qcs6125_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS6-270623/4240
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	O-QUA-QCS6-270623/4241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Product: qcs6490_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS6-270623/4242
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS6-270623/4243
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS6-270623/4244
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS6-270623/4245
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCS6-270623/4246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS6-270623/4247
Product: qcs8155_firmware					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS8-270623/4248
Product: qcs8250_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS8-270623/4249
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS8-270623/4250
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCS8-270623/4251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS8-270623/4252
Product: qcs8550_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS8-270623/4253
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS8-270623/4254
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS8-270623/4255
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS8-270623/4256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS8-270623/4257
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS8-270623/4258
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QCS8-270623/4259
Product: qfe1922_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QFE1-270623/4260
Product: qfe1952_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QFE1-270623/4261
Product: qm215_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QM21-270623/4262
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QM21-270623/4263
Product: qrb5165m_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QRB5-270623/4264
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QRB5-270623/4265
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QRB5-270623/4266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QRB5-270623/4267
Product: qrb5165n_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QRB5-270623/4268
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QRB5-270623/4269
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QRB5-270623/4270
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QRB5-270623/4271
Product: qrb5165_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QRB5-270623/4272
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QRB5-270623/4273
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QRB5-270623/4274
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QRB5-270623/4275
Product: qsm8250_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QSM8-270623/4276
Product: qsm8350_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QSM8-270623/4277
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QSM8-270623/4278
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-QSM8-270623/4279
Product: robotics_rb3_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-ROBO-270623/4280
Product: sa4150p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SA41-270623/4281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA41-270623/4282
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA41-270623/4283
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA41-270623/4284
Product: sa4155p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA41-270623/4285
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA41-270623/4286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA41-270623/4287
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA41-270623/4288
Product: sa6145p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4289
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4290
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4291
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case.	https://www.qualcomm.com/company/product-	O-QUA-SA61-270623/4292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21657	security/bulletins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4293
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4294
Product: sa6150p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4295
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4296
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4298
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4299
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4300
Product: sa6155p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4301
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4302
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while	https://www.qualcomm.com/company/product-	O-QUA-SA61-270623/4303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	security/bulletins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4304
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4305
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4306
Product: sa6155_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4307
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SA61-270623/4308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4309
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA61-270623/4310
Product: sa8145p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4311
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4312
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4314
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4315
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4316
Product: sa8150p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4317
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4318
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while	https://www.qualcomm.com/company/product-	O-QUA-SA81-270623/4319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	security/bulletins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4320
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4321
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4322
Product: sa8155p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4323
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SA81-270623/4324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4325
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4326
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4327
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4328
Product: sa8155_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4330
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4331
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4332
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4333
Product: sa8195p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4334
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while	https://www.qualcomm.com/company/product-	O-QUA-SA81-270623/4335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			querying a gsl memory node. **CVE ID : CVE-2023-21632**	security/bulletins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4336
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4337
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4338
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA81-270623/4339
Product: sa8255p_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SA82-270623/4340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA82-270623/4341
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA82-270623/4342
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA82-270623/4343
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA82-270623/4344
Product: sa8295p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA82-270623/4345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA82-270623/4346
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA82-270623/4347
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA82-270623/4348
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA82-270623/4349
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA82-270623/4350
Product: sa8540p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while	https://www.qualcomm.com/company/product-	O-QUA-SA85-270623/4351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			querying a gsl memory node. **CVE ID : CVE-2023-21632**	security/bulletins/june-2023-bulletin	
Product: sa9000p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SA90-270623/4352
Product: sc7180-ac_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC71-270623/4353
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC71-270623/4354
Product: sc7180-ad_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC71-270623/4355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC71-270623/4356
Product: sc8180x-aa_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4357
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4358
Product: sc8180x-ab_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4359
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sc8180x-ac_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4361
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4362
Product: sc8180x-ad_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4363
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4364
Product: sc8180x-af_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SC81-270623/4365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4366
Product: sc8180xp-aa_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4367
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4368
Product: sc8180xp-ab_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4369
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SC81-270623/4370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Product: sc8180xp-ac_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4371
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4372
Product: sc8180xp-ad_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4373
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4374
Product: sc8180xp-af_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4375
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4376
Product: sc8180x\+sdx55_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4377
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC81-270623/4378
Product: sc8280xp-ab_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC82-270623/4379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC82-270623/4380
Product: sc8280xp-bb_firmware					
Affected Version(s): -					
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC82-270623/4381
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SC82-270623/4382
Product: sd460_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD46-270623/4383
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD46-270623/4384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sd660_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD66-270623/4385
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD66-270623/4386
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD66-270623/4387
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD66-270623/4388
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD66-270623/4389
Product: sd662_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD66-270623/4390
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD66-270623/4391
Product: sd670_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD67-270623/4392
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD67-270623/4393
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD67-270623/4394
Product: sd675_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD67-270623/4395
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD67-270623/4396
Product: sd730_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD73-270623/4397
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD73-270623/4398
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD73-270623/4399
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending	https://www.qualcomm.com/company/	O-QUA-SD73-270623/4400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	product-security/bulletins/june-2023-bulletin	
Product: sd820_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD82-270623/4401
Product: sd821_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD82-270623/4402
Product: sd835_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD83-270623/4403
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD83-270623/4404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD83-270623/4405
Product: sd855_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD85-270623/4406
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD85-270623/4407
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD85-270623/4408
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD85-270623/4409
Product: sd865_5g_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD86-270623/4410
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD86-270623/4411
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD86-270623/4412
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD86-270623/4413
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD86-270623/4414
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SD86-270623/4415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD86-270623/4416
Product: sd888_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD88-270623/4417
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD88-270623/4418
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD88-270623/4419
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD88-270623/4420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD88-270623/4421
Product: sda845_firmware					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDA8-270623/4422
Product: sdm429w_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM4-270623/4423
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM4-270623/4424
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM4-270623/4425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM4-270623/4426
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM4-270623/4427
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM4-270623/4428
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM4-270623/4429
Product: sdm429_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM4-270623/4430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM4-270623/4431
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM4-270623/4432
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM4-270623/4433
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM4-270623/4434
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM4-270623/4435
Product: sdm439_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM4-270623/4436
Product: sdm660_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM6-270623/4437
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM6-270623/4438
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM6-270623/4439
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM6-270623/4440
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon	https://www.qualcomm.com/company/product-	O-QUA-SDM6-270623/4441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or probe-response frame. **CVE ID : CVE-2023-21661**	security/bulletins/june-2023-bulletin	
Product: sdm670_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM6-270623/4442
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM6-270623/4443
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM6-270623/4444
Product: sdm710_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM7-270623/4445
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command	https://www.qualcomm.com/company/	O-QUA-SDM7-270623/4446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	product-security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM7-270623/4447
Product: sdm712_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM7-270623/4448
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM7-270623/4449
Product: sdm845_firmware					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDM8-270623/4450
Product: sdx20m_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDX2-270623/4451
Product: sdx55_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDX5-270623/4452
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDX5-270623/4453
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDX5-270623/4454
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SDX5-270623/4455
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending	https://www.qualcomm.com/company/	O-QUA-SDX5-270623/4456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	product-security/bulletins/june-2023-bulletin	
Product: sd_455_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD_4-270623/4457
Product: sd_675_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD_6-270623/4458
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD_6-270623/4459
Product: sd_8cx_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD_8-270623/4460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628		
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD_8-270623/4461
Product: sd_8_gen1_5g_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD_8-270623/4462
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SD_8-270623/4463
Product: sg4150p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SG41-270623/4464
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SG41-270623/4465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21657	tins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SG41-270623/4466
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SG41-270623/4467
Product: sm4125_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM41-270623/4468
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM41-270623/4469
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM41-270623/4470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM41-270623/4471
Product: sm4250-aa_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM42-270623/4472
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM42-270623/4473
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM42-270623/4474
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM42-270623/4475
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	O-QUA-SM42-270623/4476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Product: sm4350-ac_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM43-270623/4477
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM43-270623/4478
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM43-270623/4479
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM43-270623/4480
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SM43-270623/4481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Product: sm4350_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM43-270623/4482
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM43-270623/4483
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM43-270623/4484
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM43-270623/4485
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM43-270623/4486
Product: sm4375_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM43-270623/4487
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM43-270623/4488
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM43-270623/4489
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM43-270623/4490
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM43-270623/4491
Product: sm4450_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM44-270623/4492
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM44-270623/4493
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM44-270623/4494
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM44-270623/4495
Product: sm6125_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM61-270623/4496
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command	https://www.qualcomm.com/company/	O-QUA-SM61-270623/4497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	product-security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM61-270623/4498
Product: sm6150-ac_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM61-270623/4499
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM61-270623/4500
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM61-270623/4501
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SM61-270623/4502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21669	tins/june-2023-bulletin	
Product: sm6225-ad_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM62-270623/4503
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM62-270623/4504
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM62-270623/4505
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM62-270623/4506
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM62-270623/4507
Product: sm6225_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM62-270623/4508
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM62-270623/4509
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM62-270623/4510
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM62-270623/4511
Product: sm6250p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM62-270623/4512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM62-270623/4513
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM62-270623/4514
Product: sm6250_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM62-270623/4515
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM62-270623/4516
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM62-270623/4517
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending	https://www.qualcomm.com/company/	O-QUA-SM62-270623/4518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	product-security/bulletins/june-2023-bulletin	
Product: sm6350_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM63-270623/4519
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM63-270623/4520
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM63-270623/4521
Product: sm6375_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM63-270623/4522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM63-270623/4523
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM63-270623/4524
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM63-270623/4525
Product: sm7125_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM71-270623/4526
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM71-270623/4527
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	O-QUA-SM71-270623/4528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM71-270623/4529
Product: sm7150-aa_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM71-270623/4530
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM71-270623/4531
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM71-270623/4532
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SM71-270623/4533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			peer with an invalid source address. **CVE ID : CVE-2023-21669**	tins/june-2023-bulletin	
Product: sm7150-ab_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM71-270623/4534
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM71-270623/4535
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM71-270623/4536
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM71-270623/4537
Product: sm7150-ac_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM71-270623/4538
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM71-270623/4539
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM71-270623/4540
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM71-270623/4541
Product: sm7225_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM72-270623/4542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM72-270623/4543
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM72-270623/4544
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM72-270623/4545
Product: sm7250-aa_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM72-270623/4546
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM72-270623/4547
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command	https://www.qualcomm.com/company/product-	O-QUA-SM72-270623/4548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM72-270623/4549
Product: sm7250-ab_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM72-270623/4550
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM72-270623/4551
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM72-270623/4552
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SM72-270623/4553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Product: sm7250-ac_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM72-270623/4554
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM72-270623/4555
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM72-270623/4556
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM72-270623/4557
Product: sm7250p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SM72-270623/4558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM72-270623/4559
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM72-270623/4560
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM72-270623/4561
Product: sm7315_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4562
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4564
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4565
Product: sm7325-ae_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4566
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4567
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4568
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	O-QUA-SM73-270623/4569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Product: sm7325-af_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4570
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4571
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4572
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4573
Product: sm7325p_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware.	https://www.qualcomm.com/company/product-	O-QUA-SM73-270623/4574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21656	security/bulletins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4575
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4576
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4577
Product: sm7325_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4578
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4580
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4581
Product: sm7350-ab_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4582
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4583
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4584
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/product-	O-QUA-SM73-270623/4585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM73-270623/4586
Product: sm8150-ac_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM81-270623/4587
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM81-270623/4588
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM81-270623/4589
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SM81-270623/4590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21669	tins/june-2023-bulletin	
Product: sm8150_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM81-270623/4591
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM81-270623/4592
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM81-270623/4593
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM81-270623/4594
Product: sm8250-ab_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SM82-270623/4595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21656	tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4596
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4597
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4598
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4599
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4600
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to	https://www.qualcomm.com/company/product-	O-QUA-SM82-270623/4601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			peer with an invalid source address. **CVE ID : CVE-2023-21669**	security/bulletins/june-2023-bulletin	
Product: sm8250-ac_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4602
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4603
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4604
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4605
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SM82-270623/4606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4607
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4608
Product: sm8250_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4609
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4610
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4612
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4613
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4614
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM82-270623/4615
Product: sm8350-ac_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM83-270623/4616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM83-270623/4617
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM83-270623/4618
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM83-270623/4619
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM83-270623/4620
Product: sm8350_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM83-270623/4621
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP	https://www.qualcomm.com/company/product-	O-QUA-SM83-270623/4622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sends input during record use case. **CVE ID : CVE-2023-21657**	security/bulletins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM83-270623/4623
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM83-270623/4624
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM83-270623/4625
Product: sm8450_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM84-270623/4626
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SM84-270623/4627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM84-270623/4628
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM84-270623/4629
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM84-270623/4630
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM84-270623/4631
Product: sm8475_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM84-270623/4632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM84-270623/4633
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM84-270623/4634
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM84-270623/4635
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SM84-270623/4636
Product: smart_audio_200_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SMAR-270623/4637
Product: smart_audio_400_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SMAR-270623/4638
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SMAR-270623/4639
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SMAR-270623/4640
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SMAR-270623/4641
Product: snapdragonwear_4100\+_platform_firmware					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4642
Product: snapdragon_210_processor_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4643
Product: snapdragon_212_mobile_platform_firmware					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4644
Product: snapdragon_630_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4645
Product: snapdragon_636_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4646
Product: snapdragon_652_mobile_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4647
Product: snapdragon_662_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4648
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4649
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4650
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4651
Product: snapdragon_675_mobile_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4652
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4653
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4654
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4655
Product: snapdragon_680_4g_mobile_platform_firmware					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4656
Product: snapdragon_690_5g_mobile_platform_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4657
Product: snapdragon_695_5g_mobile_platform_firmware					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4658
Product: snapdragon_7c\+_gen3_compute_firmware					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4659
Product: snapdragon_7c\+_gen_3_compute_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4660
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case.	https://www.qualcomm.com/company/product-	O-QUA-SNAP-270623/4661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21657	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4662
Product: snapdragon_808_processor_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4663
Product: snapdragon_810_processor_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4664
Product: snapdragon_820_automotive_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in Automotive GPU while querying a gsl memory node. **CVE ID : CVE-2023-21632**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4666
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4667
Product: snapdragon_820_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4668
Product: snapdragon_821_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4669
Product: snapdragon_835_mobile_pc_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SNAP-270623/4670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4671
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4672
Product: snapdragon_845_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4673
Product: snapdragon_850_mobile_compute_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4674
Product: snapdragon_ar2_gen1_platform_firmware					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command	https://www.qualcomm.com/company/	O-QUA-SNAP-270623/4675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	product-security/bulletins/june-2023-bulletin	
Product: snapdragon_ar2_gen_1_platform_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4676
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4677
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4678
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4679
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SNAP-270623/4680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Product: snapdragon_auto_4g_modem_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4681
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4682
Product: snapdragon_auto_5g_modem-rf_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4683
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4684
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SNAP-270623/4685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4686
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4687
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4688
Product: snapdragon_w5\+_gen1_wearable_platform_firmware					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4689
Product: snapdragon_w5\+_gen_1_wearable_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SNAP-270623/4690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21628	tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4691
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4692
Product: snapdragon_x12_lte_modem_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4693
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4694
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4695
Product: snapdragon_x20_lte_modem_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4696
Product: snapdragon_x24_lte_modem_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4697
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4698
Product: snapdragon_x50_5g_modem-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4699
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SNAP-270623/4700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4701
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4702
Product: snapdragon_x55_5g_modem-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4703
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4704
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4706
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4707
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4708
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4709
Product: snapdragon_x5_lte_modem_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4710
Product: snapdragon_x65_5g_modem-rf_system_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4711
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4712
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4713
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4714
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4715
Product: snapdragon_xr1_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4716
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4717
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4718
Product: snapdragon_xr2\+_gen1_platform_firmware					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4719
Product: snapdragon_xr2\+_gen_1_platform_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4721
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4722
Product: snapdragon_xr2_5g_platform_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4723
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4724
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4725
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/product-	O-QUA-SNAP-270623/4726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4727
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4728
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SNAP-270623/4729
Product: ssg2115p_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SSG2-270623/4730
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SSG2-270623/4731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SSG2-270623/4732
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SSG2-270623/4733
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SSG2-270623/4734
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SSG2-270623/4735
Product: ssg2125p_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SSG2-270623/4736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SSG2-270623/4737
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SSG2-270623/4738
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SSG2-270623/4739
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SSG2-270623/4740
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SSG2-270623/4741
Product: sw5100p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF	https://www.qualcomm.com/company/product-	O-QUA-SW51-270623/4742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	security/bulletins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SW51-270623/4743
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SW51-270623/4744
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SW51-270623/4745
Product: sw5100_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SW51-270623/4746
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SW51-270623/4747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SW51-270623/4748
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SW51-270623/4749
Product: sxr1120_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR1-270623/4750
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR1-270623/4751
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR1-270623/4752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sxr1230p_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR1-270623/4753
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR1-270623/4754
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR1-270623/4755
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR1-270623/4756
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR1-270623/4757
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon	https://www.qualcomm.com/company/product-	O-QUA-SXR1-270623/4758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or probe-response frame. **CVE ID : CVE-2023-21661**	security/bulletins/june-2023-bulletin	
Product: sxr2130_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR2-270623/4759
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR2-270623/4760
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR2-270623/4761
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR2-270623/4762
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SXR2-270623/4763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR2-270623/4764
Product: sxr2230p_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR2-270623/4765
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR2-270623/4766
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR2-270623/4767
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR2-270623/4768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR2-270623/4769
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-SXR2-270623/4770
Product: vision_intelligence_300_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-VISI-270623/4771
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-VISI-270623/4772
Product: vision_intelligence_400_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-VISI-270623/4773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-VISI-270623/4774
Product: wcd9326_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4775
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4776
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4777
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4778
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	O-QUA-WCD9-270623/4779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Product: wcd9330_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4780
Product: wcd9335_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4781
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4782
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4783
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command	https://www.qualcomm.com/company/product-	O-QUA-WCD9-270623/4784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4785
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4786
Product: wcd9340_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4787
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4788
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCD9-270623/4789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21657	tins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4790
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4791
Product: wcd9341_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4792
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4793
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4795
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4796
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4797
Product: wcd9360_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4798
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4799
Product: wcd9370_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4800
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4801
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4802
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4803
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4804
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCD9-270623/4805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4806
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4807
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4808
Product: wcd9371_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4809
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wcd9375_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4811
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4812
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4813
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4814
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4815
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	O-QUA-WCD9-270623/4816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4817
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4818
Product: wcd9380_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4819
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4820
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCD9-270623/4821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21657	tins/june-2023-bulletin	
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4822
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4823
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4824
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4825
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4826
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to	https://www.qualcomm.com/company/product-	O-QUA-WCD9-270623/4827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			peer with an invalid source address. **CVE ID : CVE-2023-21669**	security/bulletins/june-2023-bulletin	
Product: wcd9385_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4828
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4829
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4830
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4831
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCD9-270623/4832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21658	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4833
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4834
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4835
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCD9-270623/4836
Product: wcn3610_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4838
Product: wcn3615_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4839
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4840
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4841
Product: wcn3620_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4843
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4844
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4845
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4846
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4847
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCN3-270623/4848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21669	tins/june-2023-bulletin	
Product: wcn3660b_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4849
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4850
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4851
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4852
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4854
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4855
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4856
Product: wcn3680b_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4857
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4859
Product: wcn3680_firmware					
Affected Version(s): -					
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4860
Product: wcn3910_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4861
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4862
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4864
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4865
Product: wcn3950_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4866
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4867
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4869
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4870
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4871
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4872
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4873
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCN3-270623/4874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21669	tins/june-2023-bulletin	
Product: wcn3980_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4875
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4876
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4877
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4878
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4880
Product: wcn3988_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4881
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4882
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4883
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4885
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4886
Product: wcn3990_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4887
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4888
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4890
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4891
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4892
Product: wcn3991_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4893
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4895
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4896
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4897
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4898
Product: wcn3998_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4900
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4901
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4902
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4903
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4904
Product: wcn3999_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN3-270623/4905
Product: wcn6740_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4906
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4907
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4908
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4909
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing	https://www.qualcomm.com/company/product-	O-QUA-WCN6-270623/4910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames with missing header fields. **CVE ID : CVE-2023-21659**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4911
Product: wcn6750_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4912
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4913
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4914
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670		
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4916
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4917
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4918
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4919
Product: wcn685x-1_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4921
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4922
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4923
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4924
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4925
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCN6-270623/4926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4927
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4928
Product: wcn685x-5_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4929
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4930
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4932
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4933
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4934
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4935
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN6-270623/4936
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCN6-270623/4937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21669	tins/june-2023-bulletin	
Product: wcn785x-1_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN7-270623/4938
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN7-270623/4939
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN7-270623/4940
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN7-270623/4941
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN7-270623/4942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN7-270623/4943
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN7-270623/4944
Product: wcn785x-5_firmware					
Affected Version(s): -					
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN7-270623/4945
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN7-270623/4946
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN7-270623/4947
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the	https://www.qualcomm.com/company/product-	O-QUA-WCN7-270623/4948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received beacon or probe response frame. **CVE ID : CVE-2023-21658**	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN7-270623/4949
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN7-270623/4950
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WCN7-270623/4951
Product: wsa8810_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4952
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WSA8-270623/4953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4954
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4955
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4956
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4957
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4958
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame.	https://www.qualcomm.com/company/product-	O-QUA-WSA8-270623/4959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21661	security/bulletins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4960
Product: wsa8815_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4961
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4962
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4963
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21670		
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4965
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4966
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4967
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4968
Out-of-bounds Read	06-Jun-2023	7.5	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address. **CVE ID : CVE-2023-21669**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4969
Product: wsa8830_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4970
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4971
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4972
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4973
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4974
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WSA8-270623/4975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21659	tins/june-2023-bulletin	
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4976
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4977
Product: wsa8832_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4978
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4979
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4981
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4982
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4983
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4984
Product: wsa8835_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jun-2023	7.8	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command. **CVE ID : CVE-2023-21628**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4985
Improper Input Validation	06-Jun-2023	7.8	Memory corruption in WLAN HOST while	https://www.qualcomm.com/company/product-	O-QUA-WSA8-270623/4986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receiving an WMI event from firmware. **CVE ID : CVE-2023-21656**	security/bulletins/june-2023-bulletin	
Improper Input Validation	06-Jun-2023	7.8	Memoru corruption in Audio when ADSP sends input during record use case. **CVE ID : CVE-2023-21657**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4987
Incorrect Authorization	06-Jun-2023	7.8	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode. **CVE ID : CVE-2023-21670**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4988
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame. **CVE ID : CVE-2023-21658**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4989
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while processing frames with missing header fields. **CVE ID : CVE-2023-21659**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4990
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS in WLAN Firmware while parsing FT Information Elements. **CVE ID : CVE-2023-21660**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Jun-2023	7.5	Transient DOS while parsing WLAN beacon or probe-response frame. **CVE ID : CVE-2023-21661**	https://www.qualcomm.com/company/product-security/bulletins/june-2023-bulletin	O-QUA-WSA8-270623/4992
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 6.0					
Missing Release of Memory after Effective Lifetime	06-Jun-2023	3.3	A vulnerability was found in the pthread_create() function in libcap. This issue may allow a malicious actor to use cause __real_pthread_create() to return an error, which can exhaust the process memory. **CVE ID : CVE-2023-2602**	N/A	O-RED-ENTE-270623/4993
Affected Version(s): 7.0					
Missing Release of Memory after Effective Lifetime	06-Jun-2023	3.3	A vulnerability was found in the pthread_create() function in libcap. This issue may allow a malicious actor to use cause __real_pthread_create() to return an error, which can exhaust the process memory. **CVE ID : CVE-2023-2602**	N/A	O-RED-ENTE-270623/4994
Affected Version(s): 8.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Jun-2023	7.1	A vulnerbility was found in OpenSC. This security flaw cause a buffer overrun vulnerability in pkcs15 cardos_have_verifyrc_package. The attacker can supply a smart card package with malformed ASN1 context. The cardos_have_verifyrc_package function scans the ASN1 buffer for 2 tags, where remaining length is wrongly caculated due to moved starting pointer. This leads to possible heap-based buffer oob read. In cases where ASAN is enabled while compiling this causes a crash. Further info leak or more damage is possible. **CVE ID : CVE-2023-2977**	https://github.com/OpenSC/OpenSC/issues/2785, https://github.com/OpenSC/OpenSC/pull/2787	O-RED-ENTE-270623/4995
Missing Release of Memory after Effective Lifetime	06-Jun-2023	3.3	A vulnerability was found in the pthread_create() function in libcap. This issue may allow a malicious actor to use cause __real_pthread_create() to return an error, which can exhaust the process memory. **CVE ID : CVE-2023-2602**	N/A	O-RED-ENTE-270623/4996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.0					
Out-of-bounds Read	01-Jun-2023	7.1	A vulnerbility was found in OpenSC. This security flaw cause a buffer overrun vulnerability in pkcs15 cardos_have_verifyrc_package. The attacker can supply a smart card package with malformed ASN1 context. The cardos_have_verifyrc_package function scans the ASN1 buffer for 2 tags, where remaining length is wrongly caculated due to moved starting pointer. This leads to possible heap-based buffer oob read. In cases where ASAN is enabled while compiling this causes a crash. Further info leak or more damage is possible. **CVE ID : CVE-2023-2977**	https://github.com/OpenSC/OpenSC/issues/2785, https://github.com/OpenSC/OpenSC/pull/2787	O-RED-ENTE-270623/4997
Missing Release of Memory after Effective Lifetime	06-Jun-2023	3.3	A vulnerability was found in the pthread_create() function in libcap. This issue may allow a malicious actor to use cause __real_pthread_create() to return an error, which can exhaust the process memory.	N/A	O-RED-ENTE-270623/4998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2602		
Vendor: Samsung					
Product: exynos_5123_firmware					
Affected Version(s): -					
Incorrect Default Permissions	07-Jun-2023	9.8	An issue was discovered in the Shannon RCS component in Samsung Exynos Modem 5123 and 5300. An incorrect default permission can cause unintended querying of RCS capability via a crafted application. **CVE ID : CVE-2023-31116**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-270623/4999
Incorrect Resource Transfer Between Spheres	07-Jun-2023	9.1	An issue was discovered in the Shannon RCS component in Samsung Exynos Modem 5123 and 5300. Incorrect resource transfer between spheres can cause unintended querying of the SIM status via a crafted application. **CVE ID : CVE-2023-31114**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-270623/5000
Incorrect Resource Transfer Between Spheres	07-Jun-2023	7.5	An issue was discovered in the Shannon RCS component in Samsung Exynos Modem 5123 and 5300. Incorrect	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-270623/5001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resource transfer between spheres can cause changes to the activation mode of RCS via a crafted application. **CVE ID : CVE-2023-31115**		
Product: exynos_5300_firmware					
Affected Version(s): -					
Incorrect Default Permissions	07-Jun-2023	9.8	An issue was discovered in the Shannon RCS component in Samsung Exynos Modem 5123 and 5300. An incorrect default permission can cause unintended querying of RCS capability via a crafted application. **CVE ID : CVE-2023-31116**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-270623/5002
Incorrect Resource Transfer Between Spheres	07-Jun-2023	9.1	An issue was discovered in the Shannon RCS component in Samsung Exynos Modem 5123 and 5300. Incorrect resource transfer between spheres can cause unintended querying of the SIM status via a crafted application. **CVE ID : CVE-2023-31114**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-270623/5003
Incorrect Resource	07-Jun-2023	7.5	An issue was discovered in the	https://semiconductor.sam	O-SAM-EXYN-270623/5004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Transfer Between Spheres			Shannon RCS component in Samsung Exynos Modem 5123 and 5300. Incorrect resource transfer between spheres can cause changes to the activation mode of RCS via a crafted application. **CVE ID : CVE-2023-31115**	sung.com/support/quality-support/product-security-updates/	
Vendor: telefonica					
Product: brasil_vivo_play_firmware					
Affected Version(s): 2023.04.04.01.06.15					
Uncontrolled Recursion	05-Jun-2023	7.5	Telefnica Brasil Vivo Play (IPTV) Firmware: 2023.04.04.01.06.15 is vulnerable to Denial of Service (DoS) via DNS Recursion. **CVE ID : CVE-2023-31893**	N/A	O-TEL-BRAS-270623/5005
Vendor: Tenda					
Product: ac10_firmware					
Affected Version(s): us_ac10v4.0si_v16.03.10.13_cn					
Out-of-bounds Write	08-Jun-2023	9.8	Tenda AC10 v4 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via parameter time at /goform/saveParentControlInfo. **CVE ID : CVE-2023-34566**	N/A	O-TEN-AC10-270623/5006
Out-of-bounds Write	08-Jun-2023	6.7	Tenda AC10 v4 US_AC10V4.0si_V16.03.10.13_cn was	N/A	O-TEN-AC10-270623/5007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a stack overflow via parameter list at /goform/SetVirtualServerCfg. **CVE ID : CVE-2023-34567**		
Out-of-bounds Write	08-Jun-2023	6.7	Tenda AC10 v4 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via parameter time at /goform/PowerSaveSet. **CVE ID : CVE-2023-34568**	N/A	O-TEN-AC10-270623/5008
Out-of-bounds Write	08-Jun-2023	6.7	Tenda AC10 v4 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via parameter list at /goform/SetNetControlList. **CVE ID : CVE-2023-34569**	N/A	O-TEN-AC10-270623/5009
Out-of-bounds Write	08-Jun-2023	6.7	Tenda AC10 v4 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via parameter devName at /goform/SetOnlineDevName. **CVE ID : CVE-2023-34570**	N/A	O-TEN-AC10-270623/5010
Out-of-bounds Write	08-Jun-2023	6.7	Tenda AC10 v4 US_AC10V4.0si_V16.03.10.13_cn was	N/A	O-TEN-AC10-270623/5011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a stack overflow via parameter shareSpeed at /goform/WifiGuestSet. **CVE ID : CVE-2023-34571**		
Product: ac8_firmware					
Affected Version(s): 16.03.34.06					
Out-of-bounds Write	02-Jun-2023	9.8	Tenda AC8V4.0-V16.03.34.06 was discovered to contain a stack overflow via the timeZone parameter in the sub_44db3c function. **CVE ID : CVE-2023-33669**	N/A	O-TEN-AC8_-270623/5012
Out-of-bounds Write	02-Jun-2023	9.8	Tenda AC8V4.0-V16.03.34.06 was discovered to contain a stack overflow via the time parameter in the sub_4a79ec function. **CVE ID : CVE-2023-33670**	N/A	O-TEN-AC8_-270623/5013
Out-of-bounds Write	02-Jun-2023	9.8	Tenda AC8V4.0-V16.03.34.06 was discovered to contain a stack overflow via the deviceId parameter in the saveParentControlInfo function. **CVE ID : CVE-2023-33671**	N/A	O-TEN-AC8_-270623/5014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jun-2023	9.8	Tenda AC8V4.0-V16.03.34.06 was discovered to contain a stack overflow via the firewallEn parameter in the formSetFirewallCfg function. **CVE ID : CVE-2023-33673**	N/A	O-TEN-AC8_-270623/5015
Out-of-bounds Write	02-Jun-2023	9.8	Tenda AC8V4.0-V16.03.34.06 was discovered to contain a stack overflow via the time parameter in the get_parentControl_list_Info function. **CVE ID : CVE-2023-33675**	N/A	O-TEN-AC8_-270623/5016
Out-of-bounds Write	02-Jun-2023	7.5	Tenda AC8V4.0-V16.03.34.06 was discovered to contain a stack overflow via the shareSpeed parameter in the fromSetWifiGusetBasic function. **CVE ID : CVE-2023-33672**	N/A	O-TEN-AC8_-270623/5017
Product: g103_firmware					
Affected Version(s): 1.0.0.5					
Improper Neutralization of Special Elements used in a Command ('Comman	06-Jun-2023	8.8	There is a command injection vulnerability in the Tenda G103 Gigabit GPON Terminal with firmware version V1.0.0.5. If an attacker gains web management	N/A	O-TEN-G103-270623/5018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			privileges, they can inject commands gaining shell privileges. **CVE ID : CVE-2023-33530**		
Vendor: totolink					
Product: a7100ru_firmware					
Affected Version(s): 7.4cu.2313_b20191024					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jun-2023	9.8	TOTOLink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the staticGw parameter at /setting/setWanIeCfg. **CVE ID : CVE-2023-33556**	N/A	O-TOT-A710-270623/5019
Product: x5000r_firmware					
Affected Version(s): 9.1.0cu.2350_b20230313					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jun-2023	9.8	TOTOLINK X5000R V9.1.0cu.2350_B20230313 was discovered to contain a command injection via the setWanCfg function. **CVE ID : CVE-2023-31569**	N/A	O-TOT-X500-270623/5020
Vendor: Tp-link					
Product: tapo_c200_firmware					
Affected Version(s): 1.2.2					
Insufficiently Protected Credentials	06-Jun-2023	4.6	The AES Key-IV pair used by the TP-Link TAPO C200 camera V3 (EU) on firmware version 1.1.22 Build	N/A	O-TP--TAPO-270623/5021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			220725 is reused across all cameras. An attacker with physical access to a camera is able to extract and decrypt sensitive data containing the Wifi password and the TP-LINK account credential of the victim. **CVE ID : CVE-2023-27126**		
Product: tl-wr740n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jun-2023	8.8	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a command injection vulnerability via the component /userRpm/WlanNetworkRpm . **CVE ID : CVE-2023-33538**	N/A	O-TP--TL-W-270623/5022
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/WlanMacFilterRpm. **CVE ID : CVE-2023-33536**	N/A	O-TP--TL-W-270623/5023
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-	N/A	O-TP--TL-W-270623/5024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/FixMapCfgRpm. **CVE ID : CVE-2023-33537**		
Product: tl-wr841n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jun-2023	8.8	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a command injection vulnerability via the component /userRpm/WlanNetworkRpm . **CVE ID : CVE-2023-33538**	N/A	O-TP--TL-W-270623/5025
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/WlanMacFilterRpm. **CVE ID : CVE-2023-33536**	N/A	O-TP--TL-W-270623/5026
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component	N/A	O-TP--TL-W-270623/5027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/userRpm/FixMapCfgRpm. **CVE ID : CVE-2023-33537**		
Product: tl-wr940n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jun-2023	8.8	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a command injection vulnerability via the component /userRpm/WlanNetworkRpm . **CVE ID : CVE-2023-33538**	N/A	O-TP--TL-W-270623/5028
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/WlanMacFilterRpm. **CVE ID : CVE-2023-33536**	N/A	O-TP--TL-W-270623/5029
Out-of-bounds Read	07-Jun-2023	8.1	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/FixMapCfgRpm. **CVE ID : CVE-2023-33537**	N/A	O-TP--TL-W-270623/5030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Zyxel					
Product: lte7480-m804_firmware					
Affected Version(s): * Up to (including) 1.00\\(abra.6\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jun-2023	6.5	A buffer overflow vulnerability in the CGI program of the Zyxel NR7101 firmware versions prior to V1.00(ABUV.8)C0 could allow a remote authenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID : CVE-2023-27989**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-4g-lte-and-5g-nr-outdoor-routers	O-ZYX-LTE7-270623/5031
Product: lte7490-m904_firmware					
Affected Version(s): * Up to (including) 1.00\\(abqy.5\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jun-2023	6.5	A buffer overflow vulnerability in the CGI program of the Zyxel NR7101 firmware versions prior to V1.00(ABUV.8)C0 could allow a remote authenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID : CVE-2023-27989**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-4g-lte-and-5g-nr-outdoor-routers	O-ZYX-LTE7-270623/5032
Product: nebula_nr7101_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.15\\(accc.3\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jun-2023	6.5	A buffer overflow vulnerability in the CGI program of the Zyxel NR7101 firmware versions prior to V1.00(ABUV.8)C0 could allow a remote authenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID : CVE-2023-27989**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-4g-lte-and-5g-nr-outdoor-routers	O-ZYX-NEBU-270623/5033
Product: nr7101_firmware					
Affected Version(s): * Up to (including) 1.00\\(abuv.7\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jun-2023	6.5	A buffer overflow vulnerability in the CGI program of the Zyxel NR7101 firmware versions prior to V1.00(ABUV.8)C0 could allow a remote authenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID : CVE-2023-27989**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-4g-lte-and-5g-nr-outdoor-routers	O-ZYX-NR71-270623/5034