

National Critical Information Infrastructure Protection Centre Common Vulnerabilities and Exposures (CVE) Report 01 - 15 Jan 2025

|--|

Table of Content		
Vendor	Product	Page Number
Application		
Apache	openmeetings	1
	project_management_system	1
campcodes	school_faculty_scheduling_system	2
	student_grading_system	2
	local_storage_todo_app	3
code-projects	online_shoe_store	3
	blood_bank_management_system	4
codezips	gym_management_system	4
•	project_management_system	5
Dell	powerscale_onefs	5
emlog	emlog	6
c 1 ·	responsive_hotel_site	7
fabianros	travel_management_system	7
Fortinet	fortiproxy	7
	connect_secure	8
ivanti	neurons_for_zero-trust_access	10
	policy_secure	13
osuuu	lightpicture	14
wangl1989	mysiteforme	15
zerowdd	studentmanager	16
Hardware		
	aqt1000	17
	ar8035	17
Qualcomm	c-v2x_9150	18
	csr8811	18
	csrb31024	18

Vendor	Product	Page Number
	fastconnect_6200	18
	fastconnect_6700	19
	fastconnect_6800	20
	fastconnect_6900	20
	fastconnect_7800	22
	flight_rb5_5g	24
	immersive_home_214	24
	immersive_home_216	25
	immersive_home_316	25
	immersive_home_318	25
	immersive_home_3210	25
	immersive_home_326	26
	ipq5010	26
	ipq5028	26
Qualcomm	ipq5300	26
	ipq5302	26
	ipq5312	27
	ipq5332	27
	ipq6000	27
	ipq6010	27
	ipq6018	28
	ipq6028	28
	ipq8070a	28
	ipq8071a	28
	ipq8072a	28
	ipq8074a	29
	ipq8076	29
	ipq8076a	29
	ipq8078	29
	ipq8078a	30
	ipq8173	30
	ipq8174	30
	ipq9008	30

Vendor	Product	Page Number
	ipq9048	30
	ipq9554	31
	ipq9570	31
	ipq9574	31
	msm8996au	31
	qam8255p	32
	qam8295p	33
	qam8620p	35
	qam8650p	36
	qam8775p	37
	qamsrv1h	38
	qamsrv1m	39
	qca0000	40
	qca1062	40
Qualcomm	qca1064	41
	qca2062	41
	qca2064	41
	qca2065	42
	qca2066	42
	qca4024	42
	qca6174a	43
	qca6310	43
	qca6320	43
	qca6391	43
	qca6420	44
	qca6426	44
	qca6430	45
	qca6436	45
	qca6554a	45
	qca6564a	45
	qca6564au	46
	qca6574	47
	qca6574a	47

Vendor	Product	Page Number
	qca6574au	48
	qca6584au	49
	qca6595	50
	qca6595au	51
	qca6678aq	53
	qca6688aq	53
	qca6696	54
	qca6698aq	56
	qca6777aq	57
	qca6787aq	57
	qca6797aq	57
	qca8075	58
	qca8081	58
	qca8082	58
	qca8084	59
Qualcomm	qca8085	59
	qca8337	59
	qca8386	60
	qca9367	60
	qca9377	60
	qca9888	60
	qca9889	61
	qcc2073	61
	qcc2076	62
	qcc710	63
	qcf8000	63
	qcf8000sfp	63
	qcf8001	64
	qcm4325	64
	qcm4490	64
	qcm5430	65
	qcm6490	65
	qcm8550	66

Vendor	Product	Page Number
	qcn5022	66
	qcn5024	66
	qcn5052	67
	qcn5122	67
	qcn5124	67
	qcn5152	67
	qcn5154	68
	qcn5164	68
	qcn6023	68
	qcn6024	68
	qcn6112	68
	qcn6122	69
	qcn6132	69
	qcn6224	69
Qualcomm	qcn6274	70
	qcn6402	70
	qcn6412	71
	qcn6422	71
	qcn6432	71
	qcn7605	71
	qcn7606	72
	qcn9000	72
	qcn9012	72
	qcn9022	72
	qcn9024	73
	qcn9070	73
	qcn9072	73
	qcn9074	73
	qcn9100	74
	qcn9160	74
	qcn9274	74
	qcs410	74
	qcs4490	75

Vendor	Product	Page Number
	qcs5430	75
	qcs610	76
	qcs6490	76
	qcs7230	77
	qcs8250	77
	qcs8550	77
	qcs9100	78
	qdu1000	79
	qdu1010	79
	qdu1110	79
	qdu1210	79
	qdx1010	80
	qdx1011	80
	qep8111	80
	qfw7114	80
	qfw7124	81
_	qrb5165n	82
Qualcomm	qru1032	82
	qru1052	82
	qru1062	83
	qsm8250	83
	qxm8083	83
	robotics_rb5	83
	sa6145p	84
	sa6150p	84
	sa6155	85
	sa6155p	85
	sa7255p	86
	sa7775p	87
	sa8145p	88
	sa8150p	89
	sa8155	90
	sa8155p	90

Vendor	Product	Page Number
	sa8195p	91
	sa8255p	92
	sa8295p	94
	sa8530p	95
	sa8540p	96
	sa8620p	97
	sa8650p	98
	sa8770p	99
	sa8775p	100
	sa9000p	101
	sc8180x-aaab	103
	sc8180x-acaf	103
	sc8180x-ad	103
	sc8180xp-aaab	104
	sc8180xp-acaf	104
	sc8180xp-ad	104
	sc8180x\+sdx55	105
Qualcomm	sc8280xp-abbb	105
C	sc8380xp	105
	sd835	106
	sd865_5g	107
	sdm429w	107
	sdx55	107
	sdx65m	108
	sd_8_gen1_5g	108
	sg4150p	108
	sg8275p	108
	sm4635	109
	sm6250	109
	sm6650	110
	sm7635	110
	sm7675	110
	sm7675p	111

Vendor	Product	Page Number
	sm8550p	111
	sm8635	112
	sm8635p	113
	sm8750	113
	sm8750p	113
	snapdragon_429_mobile	113
	snapdragon_460_mobile	114
	snapdragon_480\+_5g_mobile	114
	snapdragon_480_5g_mobile	114
	snapdragon_4_gen_1_mobile	115
	snapdragon_4_gen_2_mobile	115
	snapdragon_662_mobile	115
	snapdragon_680_4g_mobile	116
	snapdragon_685_4g_mobile	116
	snapdragon_695_5g_mobile	116
Qualcomm	snapdragon_7c\+_gen_3_compute	116
	snapdragon_7c_compute_platform	117
	snapdragon_7c_gen_2_compute_platform	117
	snapdragon_820_automotive	117
	snapdragon_835_mobile_pc	118
	snapdragon_865\+_5g_mobile	118
	snapdragon_865_5g_mobile	118
	snapdragon_870_5g_mobile	119
	snapdragon_8\+_gen_1_mobile	119
	snapdragon_8\+_gen_2_mobile	119
	snapdragon_8_gen_1_mobile	120
	snapdragon_8_gen_2_mobile	120
	snapdragon_8_gen_3_mobile	121
	snapdragon_ar1_gen_1	122
	snapdragon_ar2_gen_1	122
	snapdragon_auto_4g_modem	123
	snapdragon_auto_5g_modem-rf_gen_2	123
	snapdragon_w5\+_gen_1_wearable	124

Vendor	Product	Page Number
	snapdragon_x35_5g_modem-rf	124
	snapdragon_x55_5g_modem-rf	124
	snapdragon_x65_5g_modem-rf	124
	snapdragon_x72_5g_modem-rf	125
	snapdragon_x75_5g_modem-rf	125
	snapdragon_xr2_5g	126
	srv1h	126
	srv1l	127
	srv1m	128
	ssg2115p	129
	ssg2125p	130
	sw5100	130
	sw5100p	131
	sxr1230p	131
	sxr2130	132
Qualcomm	sxr2230p	132
	sxr2250p	133
	sxr2330p	133
	talynplus	133
	video_collaboration_vc1	134
	video_collaboration_vc3	134
	video_collaboration_vc5	135
	wcd9335	135
	wcd9340	136
	wcd9341	136
	wcd9370	137
	wcd9375	138
	wcd9378	139
	wcd9380	139
	wcd9385	141
	wcd9390	143
	wcd9395	144
	wcn3620	145

Vendor	Product	Page Number
	wcn3660b	145
	wcn3680b	146
	wcn3950	146
	wcn3980	147
	wcn3988	147
	wcn3990	148
	wcn6450	148
	wcn6650	149
	wcn6740	149
	wcn6755	149
	wcn7860	150
Qualcomm	wcn7861	150
	wcn7880	150
	wcn7881	151
	wsa8810	151
	wsa8815	152
	wsa8830	153
	wsa8832	154
	wsa8835	155
	wsa8840	156
	wsa8845	158
	wsa8845h	160
Operating System		
Fortinet	fortios	162
Google	android	162
Huawei	emui	163
Huawei	harmonyos	167
Linux	linux_kernel	180
	windows_10_21h2	333
	windows_10_22h2	333
Microsoft	windows_11_22h2	334
	windows_11_23h2	334
	windows_11_24h2	335

Vendor	Product	Page Number
Microsoft	windows_server_2022_23h2	335
MICIUSUIL	windows_server_2025	336
	aqt1000_firmware	336
	ar8035_firmware	336
	c-v2x_9150_firmware	337
	csr8811_firmware	337
	csrb31024_firmware	337
	fastconnect_6200_firmware	338
	fastconnect_6700_firmware	338
	fastconnect_6800_firmware	339
	fastconnect_6900_firmware	339
	fastconnect_7800_firmware	341
	flight_rb5_5g_firmware	343
	immersive_home_214_firmware	344
	immersive_home_216_firmware	344
	immersive_home_316_firmware	344
Qualcomm	immersive_home_318_firmware	344
	immersive_home_3210_firmware	345
	immersive_home_326_firmware	345
	ipq5010_firmware	345
	ipq5028_firmware	345
	ipq5300_firmware	345
	ipq5302_firmware	346
	ipq5312_firmware	346
	ipq5332_firmware	346
	ipq6000_firmware	346
	ipq6010_firmware	347
	ipq6018_firmware	347
	ipq6028_firmware	347
	ipq8070a_firmware	347
	ipq8071a_firmware	347
	ipq8072a_firmware	348
	ipq8074a_firmware	348

Vendor	Product	Page Number
	ipq8076a_firmware	348
	ipq8076_firmware	348
	ipq8078a_firmware	349
	ipq8078_firmware	349
	ipq8173_firmware	349
	ipq8174_firmware	349
	ipq9008_firmware	349
	ipq9048_firmware	350
	ipq9554_firmware	350
	ipq9570_firmware	350
	ipq9574_firmware	350
	msm8996au_firmware	351
	qam8255p_firmware	351
	qam8295p_firmware	352
	qam8620p_firmware	354
	qam8650p_firmware	355
Qualcomm	qam8775p_firmware	356
	qamsrv1h_firmware	357
	qamsrv1m_firmware	359
	qca0000_firmware	360
	qca1062_firmware	360
	qca1064_firmware	360
	qca2062_firmware	360
	qca2064_firmware	361
	qca2065_firmware	361
	qca2066_firmware	361
	qca4024_firmware	362
	qca6174a_firmware	362
	qca6310_firmware	362
	qca6320_firmware	363
	qca6391_firmware	363
	qca6420_firmware	363
	qca6426_firmware	364

Vendor	Product	Page Number
	qca6430_firmware	364
	qca6436_firmware	364
	qca6554a_firmware	365
	qca6564au_firmware	365
	qca6564a_firmware	365
	qca6574au_firmware	366
	qca6574a_firmware	367
	qca6574_firmware	368
	qca6584au_firmware	368
	qca6595au_firmware	369
	qca6595_firmware	371
	qca6678aq_firmware	372
	qca6688aq_firmware	372
	qca6696_firmware	373
	qca6698aq_firmware	375
Qualcomm	qca6777aq_firmware	376
	qca6787aq_firmware	376
	qca6797aq_firmware	377
	qca8075_firmware	377
	qca8081_firmware	377
	qca8082_firmware	378
	qca8084_firmware	378
	qca8085_firmware	378
	qca8337_firmware	378
	qca8386_firmware	379
	qca9367_firmware	379
	qca9377_firmware	380
	qca9888_firmware	380
	qca9889_firmware	380
	qcc2073_firmware	380
	qcc2076_firmware	381
	qcc710_firmware	382
	qcf8000sfp_firmware	383

Vendor	Product	Page Number
	qcf8000_firmware	383
	qcf8001_firmware	383
	qcm4325_firmware	383
	qcm4490_firmware	384
	qcm5430_firmware	384
	qcm6490_firmware	384
	qcm8550_firmware	385
	qcn5022_firmware	386
	qcn5024_firmware	386
	qcn5052_firmware	386
	qcn5122_firmware	386
	qcn5124_firmware	386
	qcn5152_firmware	387
	qcn5154_firmware	387
Qualcomm	qcn5164_firmware	387
	qcn6023_firmware	387
	qcn6024_firmware	388
	qcn6112_firmware	388
	qcn6122_firmware	388
	qcn6132_firmware	388
	qcn6224_firmware	388
	qcn6274_firmware	389
	qcn6402_firmware	390
	qcn6412_firmware	390
	qcn6422_firmware	390
	qcn6432_firmware	390
	qcn7605_firmware	391
	qcn7606_firmware	391
	qcn9000_firmware	391
	qcn9012_firmware	391
	qcn9022_firmware	392
	qcn9024_firmware	392
	qcn9070_firmware	392

Vendor	Vendor Product			
	qcn9072_firmware	392		
	qcn9074_firmware	393		
	qcn9100_firmware	393		
	qcn9160_firmware	393		
	qcn9274_firmware	393		
	qcs410_firmware	394		
	qcs4490_firmware	394		
	qcs5430_firmware	394		
	qcs610_firmware	395		
	qcs6490_firmware	395		
	qcs7230_firmware	396		
	qcs8250_firmware	396		
	qcs8550_firmware	397		
	qcs9100_firmware	398		
	qdu1000_firmware	398		
Qualcomm	qdu1010_firmware	398		
Qualcomin	qdu1110_firmware	398		
	qdu1210_firmware	399		
	qdx1010_firmware	399		
	qdx1011_firmware	399		
	qep8111_firmware	399		
	qfw7114_firmware	400		
	qfw7124_firmware	400		
	qrb5165n_firmware	401		
	qru1032_firmware	401		
	qru1052_firmware	401		
	qru1062_firmware	402		
	qsm8250_firmware	402		
	qxm8083_firmware	402		
	robotics_rb5_firmware	402		
	sa6145p_firmware	403		
	sa6150p_firmware	403		
	sa6155p_firmware	404		

Vendor	Product	Page Number
	sa6155_firmware	405
	sa7255p_firmware	406
	sa7775p_firmware	407
	sa8145p_firmware	408
	sa8150p_firmware	408
	sa8155p_firmware	409
	sa8155_firmware	410
	sa8195p_firmware	410
	sa8255p_firmware	411
	sa8295p_firmware	413
	sa8530p_firmware	414
	sa8540p_firmware	415
	sa8620p_firmware	416
	sa8650p_firmware	417
	sa8770p_firmware	418
Qualcomm	sa8775p_firmware	419
	sa9000p_firmware	421
	sc8180x-aaab_firmware	422
	sc8180x-acaf_firmware	422
	sc8180x-ad_firmware	423
	sc8180xp-aaab_firmware	423
	sc8180xp-acaf_firmware	423
	sc8180xp-ad_firmware	424
	sc8180x\+sdx55_firmware	424
	sc8280xp-abbb_firmware	424
	sc8380xp_firmware	425
	sd835_firmware	426
	sd865_5g_firmware	426
	sdm429w_firmware	426
	sdx55_firmware	426
	sdx65m_firmware	427
	sd_8_gen1_5g_firmware	427
	sg4150p_firmware	427

Vendor	Product	Page Number
	sg8275p_firmware	428
	sm4635_firmware	428
	sm6250_firmware	428
	sm6650_firmware	429
	sm7635_firmware	429
	sm7675p_firmware	430
	sm7675_firmware	430
	sm8550p_firmware	431
	sm8635p_firmware	431
	sm8635_firmware	432
	sm8750p_firmware	432
	sm8750_firmware	432
	snapdragon_429_mobile_firmware	433
	snapdragon_460_mobile_firmware	433
	snapdragon_480\+_5g_mobile_firmware	433
Qualcomm	snapdragon_480_5g_mobile_firmware	434
	snapdragon_4_gen_1_mobile_firmware	434
	snapdragon_4_gen_2_mobile_firmware	434
	snapdragon_662_mobile_firmware	434
	snapdragon_680_4g_mobile_firmware	435
	snapdragon_685_4g_mobile_firmware	435
	snapdragon_695_5g_mobile_firmware	435
	snapdragon_7c\+_gen_3_compute_firmw are	436
	snapdragon_7c_compute_platform_firmw are	436
	snapdragon_7c_gen_2_compute_platform _firmware	436
	snapdragon_820_automotive_firmware	437
	snapdragon_835_mobile_pc_firmware	437
	snapdragon_865\+_5g_mobile_firmware	437
	snapdragon_865_5g_mobile_firmware	437
	snapdragon_870_5g_mobile_firmware	438
	snapdragon_8\+_gen_1_mobile_firmware	438
	snapdragon_8\+_gen_2_mobile_firmware	438

Vendor	Product	Page Number
	snapdragon_8_gen_1_mobile_firmware	439
	snapdragon_8_gen_2_mobile_firmware	439
	snapdragon_8_gen_3_mobile_firmware	440
	snapdragon_ar1_gen_1_firmware	441
	snapdragon_ar2_gen_1_firmware	442
	snapdragon_auto_4g_modem_firmware	442
	snapdragon_auto_5g_modem- rf_gen_2_firmware	442
	snapdragon_w5\+_gen_1_wearable_firm ware	443
	snapdragon_x35_5g_modem-rf_firmware	443
	snapdragon_x55_5g_modem-rf_firmware	443
	snapdragon_x65_5g_modem-rf_firmware	444
	snapdragon_x72_5g_modem-rf_firmware	444
	snapdragon_x75_5g_modem-rf_firmware	444
	snapdragon_xr2_5g_firmware	445
	srv1h_firmware	445
Qualcomm	srv1l_firmware	446
	srv1m_firmware	447
	ssg2115p_firmware	448
	ssg2125p_firmware	449
	sw5100p_firmware	449
	sw5100_firmware	450
	sxr1230p_firmware	450
	sxr2130_firmware	451
	sxr2230p_firmware	451
	sxr2250p_firmware	452
	sxr2330p_firmware	452
	talynplus_firmware	452
	video_collaboration_vc1_firmware	453
	video_collaboration_vc3_firmware	453
	video_collaboration_vc5_firmware	454
	wcd9335_firmware	454
	wcd9340_firmware	455

Vendor	Product Page Number		
	wcd9341_firmware	456	
	wcd9370_firmware	456	
	wcd9375_firmware	457	
	wcd9378_firmware	458	
	wcd9380_firmware	458	
	wcd9385_firmware	460	
	wcd9390_firmware	462	
	wcd9395_firmware	463	
	wcn3620_firmware	464	
	wcn3660b_firmware	464	
	wcn3680b_firmware	465	
	wcn3950_firmware	465	
	wcn3980_firmware	466	
	wcn3988_firmware	466	
Qualcomm	wcn3990_firmware	467	
	wcn6450_firmware	467	
	wcn6650_firmware	468	
	wcn6740_firmware	468	
	wcn6755_firmware	468	
	wcn7860_firmware	469	
	wcn7861_firmware	469	
	wcn7880_firmware	469	
	wcn7881_firmware	470	
	wsa8810_firmware	470	
	wsa8815_firmware	471	
	wsa8830_firmware	472	
	wsa8832_firmware	473	
	wsa8835_firmware	474	
	wsa8840_firmware	475	
	wsa8845h_firmware	477	
	wsa8845_firmware	479	

Common Vulnerabilities and Exposures (CVE) Report						
Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			Application			
Vendor: Apa	iche					
Product: op	enmeetings					
Affected Vers	sion(s): From (in	cluding) 2	.1 Up to (excluding) 8.0.0			
			Vendor: The Apache Software Foundation			
			Versions Affected: Apache OpenMeetings from 2.1.0 before 8.0.0			
Deserializati on of Untrusted Data	08-Jan-2025	9.8	Description: Default clustering instructions at https://openmeetings.apac he.org/Clustering.html doe sn't specify white/black lists for OpenJPA this leads to possible deserialisation of untrusted data. Users are recommended to upgrade to version 8.0.0 and update their startup scripts to include the relevant 'openjpa.serialization.class. blacklist' and 'openjpa.serialization.class. whitelist' configurations as shown in the documentation.	https://lists.apa che.org/thread/ o0k05jxrt5tp4n m45lj14yfjxmg6 7m95	A-APA-OPEN- 200125/1	
Vendor: can	ncodos		CVE ID: CVE-2024-54676			
	oject_managemo	ant evetor	n			
Affected Vers	, 0	Jit_Systel				
Improper Access Control	04-Jan-2025	6.3	A vulnerability was found in Campcodes Project Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /forms/update_forms.php? action=change_pic2&id=4.	N/A	A-CAM-PROJ- 200125/2	

CVSSv3 Scoring Scale
* stands for all versions

5-6

6-7

7-8

9-10

3-4

Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') External Control of File Name or Path O4-Jan-2025 O4-Jan-2025 7.3 7.3 Vulnerability is an unknown functionality of the file /admin/ajax.php?action=log jin. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2025-0210 A vulnerability is an unknown functionality of the gile /admin/ajax.php?action=log jin. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The manipulation of the argument page leads to file inclusion. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2025-0211	NCIIPC ID	Patch	Description & CVE ID	CVSSv3	Publish Date	Weakness
A vulnerability has been found in Campcodes School Faculty Scheduling System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/ajax.php?action=lo gin. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2025-0210 A vulnerability was found in Campcodes School Faculty Scheduling System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/index.php. The manipulation of the argument page leads to file inclusion. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2025-0211			unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public			
Affected Version(s): 1.0 A vulnerability has been found in Campcodes School Faculty Scheduling System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/ajax.php?action=lo gin. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2025-0210 A vulnerability has been found in Campcodes School Faculty Scheduling System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/index.php. The manipulation of the argument page leads to file inclusion. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2025-0211			CVE ID: CVE-2025-0213			
A vulnerability has been found in Campcodes School Faculty Scheduling System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/ajax.php?action=lo gin. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2025-0210 External Control of File Name or Path O4-Jan-2025 6.3 A vulnerability has been found in Campcodes School Faculty Scheduling System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/index.php. The manipulation of the argument page leads to file inclusion. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2025-0211			stem	eduling_s	ool_faculty_sch	Product: sch
found in Campcodes School Faculty Scheduling System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/ajax.php?action=lo gin. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2025-0210 A vulnerability was found in Campcodes School Faculty Scheduling System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/index.php. The manipulation of the argument page leads to file inclusion. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2025-0210					ion(s): 1.0	Affected Vers
External Control of File Name or Path A vulnerability was found in Campcodes School Faculty Scheduling System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/index.php. The manipulation of the argument page leads to file inclusion. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	A-CAM-SCHO- 200125/3	N/A	found in Campcodes School Faculty Scheduling System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/ajax.php?action=lo gin. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and	7.3	04-Jan-2025	Improper Neutralizati on of Special Elements in Output Used by a Downstream Component ('Injection')
External Control of File Name or Path O4-Jan-2025 Campcodes School Faculty Scheduling System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/index.php. The manipulation of the argument page leads to file inclusion. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2025-0211			CVE ID: CVE-2025-0210			
	A-CAM-SCHO- 200125/4	N/A	Campcodes School Faculty Scheduling System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/index.php. The manipulation of the argument page leads to file inclusion. The attack may be launched remotely. The exploit has been disclosed to the public and may be	6.3	04-Jan-2025	Control of File Name or
Product: student grading system			CVE ID: CVE-2025-0211			
				stem	dent_grading_sy	Product: stu
Affected Version(s): 1.0					ion(s): 1.0	Affected Vers
Improper Neutralizati 04-Jan-2025 On of Special A vulnerability was found in Campcodes Student Grading System 1.0. It has been	A-CAM-STUD- 200125/5	N/A	Campcodes Student Grading	6.3	04-Jan-2025	Neutralizati

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			classified as critical. This affects an unknown part of the file /view_students.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. CVE ID: CVE-2025-0212		
Vendor: cod	e-projects				
Product: loc	al_storage_todo	_app			
Affected Vers	sion(s): 1.0				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2025	2.4	A vulnerability has been found in code-projects Local Storage Todo App 1.0 and classified as problematic. This vulnerability affects unknown code of the file /js-todo-app/index.html. The manipulation of the argument Add leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	N/A	A-COD-LOCA- 200125/6
			CVE ID: CVE-2025-0228		
Product: onl	line_shoe_store				
Affected Vers	sion(s): 1.0				
Improper Neutralizati on of Special Elements in Output Used by a Downstream Component ('Injection')	04-Jan-2025	7.3	A vulnerability, which was classified as critical, has been found in code-projects Online Shoe Store 1.0. Affected by this issue is some unknown functionality of the file /function/login.php. The manipulation of the argument password leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	N/A	A-COD-ONLI- 200125/7

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-0207		
Improper Neutralizati on of Special Elements in Output Used by a Downstream Component ('Injection')	04-Jan-2025	6.3	A vulnerability, which was classified as critical, was found in code-projects Online Shoe Store 1.0. This affects an unknown part of the file /summary.php. The manipulation of the argument tid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2025-0208	N/A	A-COD-ONLI- 200125/8
Vendor: cod	ezips				
Product: blo	od_bank_manag	gement_sy	ystem		
Affected Vers	sion(s): 1.0				
Improper Neutralizati on of Special Elements in Output Used by a Downstream Component ('Injection')	05-Jan-2025	6.3	A vulnerability was found in Codezips Blood Bank Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /successadmin.php. The manipulation of the argument psw leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2025-0232	N/A	A-COD-BLOO- 200125/9
Product: gvr	n_management_	system			
Affected Vers		- <i>J</i>			
Improper Neutralizati on of Special Elements in Output Used by a Downstream Component ('Injection')	05-Jan-2025	6.3	A vulnerability has been found in Codezips Gym Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /dashboard/admin/submit_payments.php. The	N/A	A-COD-GYM 200125/10

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument m_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
			CVE ID: CVE-2025-0231		
Product: pro	oject_manageme	nt_syster	n		
Affected Vers	sion(s): 1.0				
Improper Neutralizati on of Special Elements in Output Used by a Downstream Component ('Injection')	05-Jan-2025	7.3	A vulnerability was found in Codezips Project Management System 1.0. It has been classified as critical. This affects an unknown part of the file /pages/forms/course.php. The manipulation of the argument course_name leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2025-0233	N/A	A-COD-PROJ- 200125/11
Vendor: Dell					
Product: pov	werscale_onefs				
Affected Vers	sion(s): From (inc	cluding) 8.	2.2 Up to (excluding) 9.4.0.2	0	
Incorrect Permission Assignment for Critical Resource	06-Jan-2025	5	Dell PowerScale OneFS 8.2.2.x through 9.8.0.x contains an incorrect permission assignment for critical resource vulnerability. A locally authenticated attacker could potentially exploit this vulnerability, leading to denial of service. CVE ID: CVE-2024-47475	https://www.de ll.com/support/ kbdoc/en- us/000242681/ dsa-2024-417- security-update- for-dell- powerscale- onefs-for- security- vulnerability	A-DEL-POWE- 200125/12
Affected Vers	sion(s): From (inc	cluding) 9	5.0.0 Up to (including) 9.5.0	.8	l
Incorrect Permission Assignment for Critical Resource	06-Jan-2025	5	Dell PowerScale OneFS 8.2.2.x through 9.8.0.x contains an incorrect permission assignment for critical resource	https://www.de ll.com/support/ kbdoc/en- us/000242681/ dsa-2024-417-	A-DEL-POWE- 200125/13

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. A locally authenticated attacker could potentially exploit this vulnerability, leading to denial of service. CVE ID: CVE-2024-47475	security-update- for-dell- powerscale- onefs-for- security- vulnerability	
Affected Vers	sion(s): From (inc	cluding) 9.	6.0 Up to (including) 9.7.0.3		
Incorrect Permission Assignment for Critical Resource	06-Jan-2025	5	Dell PowerScale OneFS 8.2.2.x through 9.8.0.x contains an incorrect permission assignment for critical resource vulnerability. A locally authenticated attacker could potentially exploit this vulnerability, leading to denial of service.	https://www.de ll.com/support/ kbdoc/en- us/000242681/ dsa-2024-417- security-update- for-dell- powerscale- onefs-for- security-	A-DEL-POWE- 200125/14
A.CC		1 11 20	CVE ID: CVE-2024-47475	vulnerability	
Affected Vers	sion(s): From (inc	ciuding) 9.	8.0.0 Up to (including) 9.8.0.	L	I
Incorrect Permission Assignment for Critical Resource	06-Jan-2025	5	Dell PowerScale OneFS 8.2.2.x through 9.8.0.x contains an incorrect permission assignment for critical resource vulnerability. A locally authenticated attacker could potentially exploit this vulnerability, leading to denial of service. CVE ID: CVE-2024-47475	https://www.de ll.com/support/ kbdoc/en- us/000242681/ dsa-2024-417- security-update- for-dell- powerscale- onefs-for- security- vulnerability	A-DEL-POWE- 200125/15
W J1	"		CVE ID. CVE-2024-47473	vumerability	
Vendor: eml					
Product: em		11	40 Harta (1: -1 -1: -1: -1: -1: -1: -1: -1: -1: -1		
Affected Vers	sion(s): From (inc	ciuaing) 2.	4.0 Up to (including) 2.4.3		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2025	3.5	A vulnerability classified as problematic has been found in Emlog Pro up to 2.4.3. Affected is an unknown function of the file /admin/article.php?action= upload_cover of the component Cover Upload Handler. The manipulation of the argument image leads to cross site scripting. It is possible to launch the	N/A	A-EML-EMLO- 200125/16

0-1

5-6

6-7

7-8

9-10

3-4

	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack remotely. The exploit has been disclosed to the public and may be used.		
			CVE ID: CVE-2024-13140		
Vendor: fab	ianros				
Product: res	sponsive_hotel_s	ite			
Affected Vers	sion(s): 1.0				
Improper Neutralizati on of Special Elements in Output Used by a Downstream Component ('Injection')	05-Jan-2025	6.3	A vulnerability, which was classified as critical, was found in code-projects Responsive Hotel Site 1.0. Affected is an unknown function of the file /admin/print.php. The manipulation of the argument pid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2025-0230	N/A	A-FAB-RESP- 200125/17
Product: tra	vvol managaman				
1 Toudett tla	vel_managemer	it_system			
Affected Vers		it_system			
		6.3	A vulnerability, which was classified as critical, has been found in code-projects Travel Management System 1.0. This issue affects some unknown processing of the file /enquiry.php. The manipulation of the argument pid/t1/t2/t3/t4/t5/t6/t7 leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2025-0229	N/A	A-FAB-TRAV- 200125/18
Affected Versilians Improper Neutralizati on of Special Elements in Output Used by a Downstream Component	osion(s): 1.0 05-Jan-2025		A vulnerability, which was classified as critical, has been found in code-projects Travel Management System 1.0. This issue affects some unknown processing of the file /enquiry.php. The manipulation of the argument pid/t1/t2/t3/t4/t5/t6/t7 leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	N/A	A-FAB-TRAV- 200125/18

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
a v bb v b bcor mg bcare	0 1		_ 0	0 1	1 0	0 0	0 ,	, 0		7 10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticati on Bypass Using an Alternate Path or Channel	14-Jan-2025	9.8	An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] affecting FortiOS version 7.0.0 through 7.0.16 and FortiProxy version 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12 allows a remote attacker to gain super-admin privileges via crafted requests to Node.js websocket module. CVE ID: CVE-2024-55591	https://fortigua rd.fortinet.com/ psirt/FG-IR-24- 535	A-FOR-FORT- 200125/19
Affected Vers	sion(s): From (inc	cluding) 7.	2.0 Up to (excluding) 7.2.13		
Authenticati on Bypass Using an Alternate Path or Channel	14-Jan-2025	9.8	An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] affecting FortiOS version 7.0.0 through 7.0.16 and FortiProxy version 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12 allows a remote attacker to gain super-admin privileges via crafted requests to Node.js websocket module. CVE ID: CVE-2024-55591	https://fortigua rd.fortinet.com/ psirt/FG-IR-24- 535	A-FOR-FORT- 200125/20
Vendor: ivar	nti		CVEID. CVE 2021 33371		
Product: cor					
	sion(s): * Up to (e	excluding)	9.1		
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges.	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	A-IVA-CONN- 200125/21
Affected Vers	sion(s): 21.12				
Interior vers					

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. CVE ID: CVE-2025-0283	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	A-IVA-CONN- 200125/22
Affected Vers	sion(s): 21.9				
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. CVE ID: CVE-2025-0283	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	A-IVA-CONN- 200125/23
Affected Vers	sion(s): 22.1				
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. CVE ID: CVE-2025-0283	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	A-IVA-CONN- 200125/24
Affected Vers	sion(s): 22.7				
Stack-based Buffer Overflow	08-Jan-2025	9	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways-	A-IVA-CONN- 200125/25

0-1

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before version 22.7R2.3 allows a remote unauthenticated attacker to achieve remote code execution. CVE ID: CVE-2025-0282	CVE-2025-0282- CVE-2025-0283	
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. CVE ID: CVE-2025-0283	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	A-IVA-CONN- 200125/26
Affected Vers	ion(s): 9.1				
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges.	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	A-IVA-CONN- 200125/27
ACC . LYY	. () .	1 1: 20:	CVE ID: CVE-2025-0283		
Affected Vers	ion(s): From (inc	cluding) 22	2.2 Up to (excluding) 22.7		
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. CVE ID: CVE-2025-0283	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	A-IVA-CONN- 200125/28

CVSSv3 Scoring Scale
* stands for all versions 3-4 2-3 5-6 7-8 9-10

Affected Vers	ion(s): -				
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges.	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	A-IVA-NEUR- 200125/29
Affected Vers	ion(s): 22.2				
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. CVE ID: CVE-2025-0283	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	A-IVA-NEUR- 200125/30
Affected Vers	ion(s): 22.3				
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges.	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	A-IVA-NEUR- 200125/31
			CVE ID: CVE-2025-0283		
Affected Vers	ion(s): 22.4				
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure-	A-IVA-NEUR- 200125/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. CVE ID: CVE-2025-0283	ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	
Affected Vers	sion(s): 22.5		CVE 1D. CVE 2023 0203		
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. CVE ID: CVE-2025-0283	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	A-IVA-NEUR- 200125/33
Affected Vers	sion(s): 22.6				
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges.	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	A-IVA-NEUR- 200125/34
			CVE ID: CVE-2025-0283		
Stack-based Buffer Overflow	08-Jan-2025	9	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a remote unauthenticated attacker to achieve remote code execution. CVE ID: CVE-2025-0282	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	A-IVA-NEUR- 200125/35
Stack-based	08-Jan-2025	7	A stack-based buffer	https://forums.i	A-IVA-NEUR-

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. CVE ID: CVE-2025-0283	vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	200125/36
Product: po	licv secure				
•	$\frac{1}{\sin(s)}$: * Up to (ϵ	excluding)	22.7		
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. CVE ID: CVE-2025-0283	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	A-IVA-POLI- 200125/37
Stack-based Buffer Overflow	08-Jan-2025	9	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a remote unauthenticated attacker to achieve remote code execution.	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	A-IVA-POLI- 200125/38
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated	https://forums.i vanti.com/s/arti cle/Security- Advisory-Ivanti- Connect-Secure- Policy-Secure- ZTA-Gateways- CVE-2025-0282- CVE-2025-0283	A-IVA-POLI- 200125/39

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			attacker to escalate their privileges.				
			CVE ID: CVE-2025-0283				
Vendor: osu	uu						
Product: lightpicture							
Affected Vers	ion(s): 1.2.0						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2025	3.5	A vulnerability classified as problematic was found in osuuu LightPicture up to 1.2.2. This vulnerability affects unknown code of the file /api/upload of the component SVG File Upload Handler. The manipulation of the argument file leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	N/A	A-OSU-LIGH- 200125/40		
			CVE ID: CVE-2024-13141				
Affected Vers	ion(s): 1.2.1				1		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2025	3.5	A vulnerability classified as problematic was found in osuuu LightPicture up to 1.2.2. This vulnerability affects unknown code of the file /api/upload of the component SVG File Upload Handler. The manipulation of the argument file leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2024-13141	N/A	A-OSU-LIGH- 200125/41		
Affected Vers	ion(s): 1.2.2						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	05-Jan-2025	3.5	A vulnerability classified as problematic was found in osuuu LightPicture up to 1.2.2. This vulnerability affects unknown code of the file /api/upload of the component SVG File Upload	N/A	A-OSU-LIGH- 200125/42		

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')			Handler. The manipulation of the argument file leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2024-13141		
Vendor: wa	ngl1989				
Product: my	siteforme				
Affected Vers	sion(s): 1.0				
Server-Side Request Forgery (SSRF)	05-Jan-2025	6.3	A vulnerability was found in wangl1989 mysiteforme 1.0. It has been rated as critical. This issue affects the function doContent of the file src/main/java/com/mysite form/admin/controller/sys tem/FileController. The manipulation of the argument content leads to server-side request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	N/A	A-WAN-MYSI- 200125/43
			CVE ID: CVE-2024-13139		
Improper Input Validation	05-Jan-2025	6.3	A vulnerability was found in wangl1989 mysiteforme 1.0 and classified as critical. Affected by this issue is the function rememberMeManager of the file src/main/java/com/mysite forme/admin/config/Shiro Config.java. The manipulation leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID: CVE-2024-13136	N/A	A-WAN-MYSI- 200125/44
Improper	05-Jan-2025	4.7		N/A	A-WAN-MYSI-
mproper	U5-Jan-2025	4./	A vulnerability was found in	N/A	A-WAN-MYSI-

CV35V3 SCOTTING Scale 0-1 1-2 2-3 3-4 4-3 3-0 0-7 7-0 0-9 9-1		CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
---	--	----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Access Control			wangl1989 mysiteforme 1.0. It has been declared as critical. This vulnerability affects the function upload of the file src/main/java/com/mysite form/admin/service/ipl/Lo calUploadServiceImpl. The manipulation of the argument test leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		200125/45			
			CVE ID: CVE-2024-13138					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2025	2.4	A vulnerability was found in wangl1989 mysiteforme 1.0. It has been classified as problematic. This affects the function RestResponse of the file src/main/java/com/mysite forme/admin/controller/sy stem/SiteController. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	N/A	A-WAN-MYSI- 200125/46			
			CVE ID: CVE-2024-13137					
Vendor: zerowdd								
Product: stu	dentmanager							
Affected Vers	ion(s): 1.0							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2025	2.4	A vulnerability was found in ZeroWdd studentmanager 1.0. It has been declared as problematic. This vulnerability affects the function submitAddRole of the file src/main/java/com/zero/s ystem/controller/RoleCont roller. java. The manipulation of the argument name leads to cross site scripting. The	N/A	A-ZER-STUD- 200125/47			

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			attack can be initiated remotely.			
			CVE ID: CVE-2024-13142			
			Hardware			
Vendor: Qua	alcomm					
Product: aqt	1000					
Affected Vers	sion(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-AQT1- 200125/48	
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-AQT1- 200125/49	
Overflow')	2025			bulletin.html		
Product: ar8						
Affected Vers	Sion(s): -		Momory corruption can			
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-AR80- 200125/50	
			CVE ID: CVE-2024-45553			
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-AR80- 200125/51	
			CVE ID: CVE-2024-45558	bulletin.html		
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every	https://docs.qu alcomm.com/pr oduct/publicres ources/security	H-QUA-AR80- 200125/52	

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			valid opcode received from sound model driver.	bulletin/january -2025-		
			CVE ID: CVE-2024-33067	bulletin.html		
Product: c-v	2x 9150					
Affected Vers						
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-C-V2- 200125/53	
Product: csr	8811					
Affected Vers	sion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-CSR8- 200125/54	
Product: csr	b31024					
Affected Vers	sion(s): -					
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-CSRB- 200125/55	
			CVE ID: CVE-2024-33067	bulletin.html		
	tconnect_6200					
Affected Vers	sion(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/56	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-FAST- 200125/57	

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	ources/security bulletin/january -2025- bulletin.html		
			CVE ID: CVE-2024-45553			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/58	
Product: fas	tconnect_6700					
Affected Vers	sion(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/59	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/60	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/61	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/62	
Ruffon Orran	06 Ian 2025	7.5		https://docs.cv	н она баст	
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	H-QUA-FAST-	

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/63
Product: fast	tconnect_6800				
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/64
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/65
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-FAST- 200125/66
			CVE ID: CVE-2024-33067	bulletin.html	
	tconnect_6900				
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/67
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/68
Overnow j					

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/69
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/70
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. CVE ID: CVE-2024-45548	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/71
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. CVE ID: CVE-2024-45550	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/72
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/73
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/74
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-FAST- 200125/75

0-1

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID: CVE-2024-45558	bulletin.html		
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/76	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/77	
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/78	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-FAST- 200125/79	
D 1 . C	. =000		CVE ID: CVE-2024-33067	bulletin.html		
	tconnect_7800					
Affected Vers	sion(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/80	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/81	
Buffer Copy without Checking	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-FAST- 200125/82	

CVSSv3 Scoring Scale
* stands for all versions

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	ources/security bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/83
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/84
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. CVE ID: CVE-2024-45550	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/85
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. CVE ID: CVE-2024-45548	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/86
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/87
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/88

5-6

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID: CVE-2024-45558			
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/89	
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/90	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/91	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FAST- 200125/92	
Product: flig	ht rb5 5g			Surremmenn		
Affected Vers						
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-FLIG- 200125/93	
Product: im	mersive_home_2	214				
Affected Vers	ion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-IMME- 200125/94	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	ources/security bulletin/january -2025- bulletin.html		
Product: im	mersive_home_2	216				
Affected Vers						
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IMME- 200125/95	
Product: im	mersive_home_3	316				
Affected Vers	sion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IMME- 200125/96	
Product: im	mersive_home_3	318				
Affected Vers	sion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-IMME- 200125/97	
D		2240	CVE ID: CVE-2024-45558	bulletin.html		
	mersive_home_3	5210				
Affected Vers	oron(s): -		Transient DOS can occur			
Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IMME- 200125/98	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: imi	nersive_home_3	326			
Affected Vers	ion(s): -				
Buffer Over- read 06-Jan-2025		7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-IMME- 200125/99
			CVE ID: CVE-2024-45558	bulletin.html	
Product: ipq	5010				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ5- 200125/100
Product: ipq	5028				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ5- 200125/101
Product: ipq	5300				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ5- 200125/102
Product: ipq	5302				
Affected Vers	<u> </u>				
	ion(s)		Transient DOS can occur	https://docs.gv	
Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-IPQ5- 200125/103

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	ources/security bulletin/january -2025- bulletin.html		
Product: ipq	5312					
Affected Vers	sion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ5- 200125/104	
Product: ipq	5332					
Affected Vers	sion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ5- 200125/105	
Product: ipq	6000					
Affected Vers	sion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-IPQ6- 200125/106	
			CVE ID: CVE-2024-45558	bulletin.html		
Product: ipq						
Affected Vers	sion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ6- 200125/107	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq	6018				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-IPQ6- 200125/108
			CVE ID: CVE-2024-45558	bulletin.html	
Product: ipq	6028				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ6- 200125/109
Product: ipq	8070a				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ8- 200125/110
Product: ipq	8071a				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ8- 200125/111
Product: ipq	8072a				
Affected Vers					
Allected VelS	ion(s)		Transient DOC can accur	https://dogg.go	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-IPQ8- 200125/112

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	ources/security bulletin/january -2025- bulletin.html	
Product: ipq	8074a				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ8- 200125/113
Product: ipq	8076				l
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ8- 200125/114
Product: ipq	8076a				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-IPQ8- 200125/115
			CVE ID: CVE-2024-45558	bulletin.html	
Product: ipq					
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ8- 200125/116

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq	8078a				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-IPQ8- 200125/117
			CVE ID: CVE-2024-45558	bulletin.html	
Product: ipq	8173				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ8- 200125/118
Product: ipq	8174				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ8- 200125/119
Product: ipq	9008				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ9- 200125/120
Product: ipq	9048				
Affected Vers	·				
	ion(s).		Transient DOS can occur	https://docs.gv	
Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-IPQ9- 200125/121

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	ources/security bulletin/january -2025- bulletin.html	
Product: ipq	9554				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ9- 200125/122
Product: ipq	9570				
Affected Vers					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ9- 200125/123
Product: ipq	9574				l
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-IPQ9- 200125/124
Product: ms	m8996au		0.2.2.0.2.2021		
Affected Vers					
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-MSM8- 200125/125

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			image.		
			CVE ID: CVE-2024-45555		
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-MSM8- 200125/126
Product: qar	n8255p				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/127
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/128
			CVE ID: CVE-2024-45553		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/129
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QAM8- 200125/130

5-6

6-7

7-8

9-10

3-4

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		CVE ID: CVE-2024-45558	bulletin.html	
06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/131
06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/132
06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/133
n8295p				l
ion(s): -				
06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/134
		CVE ID: CVE-2024-45555		
06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/135
		Uncontrolled resource	https://docs.qu	H-QUA-QAM8-
	06-Jan-2025 06-Jan-2025 06-Jan-2025 06-Jan-2025	06-Jan-2025 6.1 06-Jan-2025 5.5 n8295p ion(s): - 06-Jan-2025 8.4	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/137
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/138
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/139
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/140
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/141
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/142
Buffer Over-	06-Jan-2025	5.5	Transient DOS can occur	https://docs.qu	H-QUA-QAM8-

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when GVM sends a specific message type to the Vdev-FastRPC backend.	alcomm.com/pr oduct/publicres ources/security bulletin/january	200125/143
			CVE ID: CVE-2024-45559	-2025- bulletin.html	
Product: qar	n8620p				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/144
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/145
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QAM8- 200125/146
			CVE ID: CVE-2024-45558	bulletin.html	
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/147
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-QAM8- 200125/148

CVSSv3 Scoring Scale
* stands for all versions

5-6

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FastRPC backend. CVE ID: CVE-2024-45559	ources/security bulletin/january -2025- bulletin.html	
Product: qar					
Affected Vers	ion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/149
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/150
			CVE ID: CVE-2024-45553		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/151
			Transient DOS can occur		
Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QAM8- 200125/152
			CVE ID: CVE-2024-45558	bulletin.html	
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	H-QUA-QAM8- 200125/153

CVSSv3 Scoring Scale
* stands for all versions

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-23366	-2025- bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/154
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/155
Product: qai	m8775p				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/156
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/157
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/158
N/A	06-Jan-2025	7.5	Uncontrolled resource	https://docs.qu	H-QUA-QAM8-

CVSSv3 Scoring Scale
* stands for all versions

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/159
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/160
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/161
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAM8- 200125/162
Product: qai	msrv1h				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAMS- 200125/163
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAMS- 200125/164

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arise.		
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAMS- 200125/165
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAMS- 200125/166
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAMS- 200125/167
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAMS- 200125/168
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAMS- 200125/169
Product: qar	nsrv1m				
Affected Vers	ion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAMS- 200125/170
CVSSv3 Scoring	Scale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tampered IFS2 system image.		
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAMS- 200125/171
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAMS- 200125/172
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAMS- 200125/173
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QAMS- 200125/174
Product: qca	0000			bunetiii.iitiiii	
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA0- 200125/175
Product: qca	1062				

CVSSv3 Scoring Scale
* stands for all versions 2-3 3-4 5-6 6-7 7-8 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA1- 200125/176
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA1- 200125/177
Product: qca	1064				
Affected Vers	ion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCA1- 200125/178
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA1- 200125/179
Product: qca	2062				
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA2- 200125/180
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA2- 200125/181
Product: qca	2064				

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	ion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA2- 200125/182
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA2- 200125/183
Product: qca	2065				
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA2- 200125/184
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA2- 200125/185
Product: qca	2066				
Affected Vers	ion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA2- 200125/186
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA2- 200125/187
Product: qca	4024				

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA4- 200125/188
Product: qca	a6174a				1
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/189
			CVE ID: CVE-2024-45553		
Product: qca					
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/190
Product: qca	a6320				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/191
Product: qca	a6391				
Affected Vers					
			Memory corruption can	https://docs.qu	H-QUA-QCA6-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45553		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/193
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/194
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/195
Product: qca	6420		CVE ID: CVE-2024-33007	buneun.num	
Affected Vers					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/196
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/197
Product: qca					
Affected Vers	ion(s): -				

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/198
Product: qca	6430				
Affected Vers					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/199
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/200
Product: qca	6436				l
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCA6- 200125/201
			CVE ID: CVE-2024-33067	bulletin.html	
Product: qca	6554a				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCA6- 200125/202
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qca	6564a				
Affected Vers	ion(s): -				

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
a v bb v b b cor mg b care	0 1			0 1	1.0	0 0	0 /	, 0	0)	7 20

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/203
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/204
Product: qca	16564au				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/205
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/206
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/207

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca	16574			ı	
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/208
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/209
Product: qca	16574a				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	H-QUA-QCA6- 200125/210
			tampered IFS2 system image. CVE ID: CVE-2024-45555	-2025- bulletin.html	
Use After Free	06-Jan-2025	7.8	tampered IFS2 system image.		H-QUA-QCA6- 200125/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	ources/security bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/213
Product: qca	 16574au				
Affected Vers					
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/214
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/215
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/216
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the	https://docs.qu alcomm.com/pr oduct/publicres ources/security	H-QUA-QCA6- 200125/217

0-1

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global registers through SMMU. CVE ID: CVE-2024-43064	bulletin/january -2025- bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/218
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/219
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/220
Product: qca	16584au				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/221
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/222

0-1

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/223
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/224
Product: qca	16595				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/225
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/226
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/228
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/229
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/230
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCA6- 200125/231
Product: qca	16595au			bulletin.html	
Affected Vers	ion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/232
			CVE ID: CVE-2024-45555		
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	H-QUA-QCA6- 200125/233

CVSSv3 Scoring Scale
* stands for all versions

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45542	-2025- bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/234
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/235
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/236
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/237
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/238
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/239

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

YAY 7	n 1	OVICE C	B 1 .1 2 2	n . 1	Nove a
Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/240
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/241
Product: qca	16678aq				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/242
Product: qca	16688ag				
Affected Vers					
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/243
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/244

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
weakiless	Publish Date	CVSSVS	-	Pattii	NCIIPCID
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/245
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/246
Product: qca	16696				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/247
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/248
			CVE ID: CVE-2024-45553		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/249
	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	H-QUA-QCA6-

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/250
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/251
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/252
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/253
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/254
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/255
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/256

CVSSv3 Scoring Scale
* stands for all versions 3-4 9-10 0-1 2-3 4-5 5-6 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca	16698aq				
Affected Vers	ion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/257
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/258
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/259
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/260
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/261
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback	https://docs.qu alcomm.com/pr	H-QUA-QCA6- 200125/262

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/263
Product: qca	6777aq				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/264
Product: qca	6787aq				
Affected Vers	-				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/265
Product: qca	6797aq				
Affected Vers	_				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA6- 200125/266
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	H-QUA-QCA6-

0-1

5-6

6-7

7-8

9-10

3-4

read Product: qca	9075		when the driver parses the per STA profile IE and tries to access the EXTN element	alcomm.com/pr oduct/publicres	200125/267
Product: qca	907F		ID without checking the IE length. CVE ID: CVE-2024-45558	ources/security bulletin/january -2025- bulletin.html	
	100/5				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCA8- 200125/268
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qca					
Affected Vers	ion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA8- 200125/269
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA8- 200125/270
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA8- 200125/271
Product: qca	8082				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA8- 200125/272
Product: qca	8084				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCA8- 200125/273
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qca	18085				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCA8- 200125/274
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qca	18337				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA8- 200125/275
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	H-QUA-QCA8- 200125/276

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length. CVE ID: CVE-2024-45558	-2025- bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCA8- 200125/277
			CVE ID: CVE-2024-33067	bulletin.html	
Product: qca					
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA8- 200125/278
Product: qca	9367				
Affected Vers					
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA9- 200125/279
Product: qca	9377				l
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCA9- 200125/280
_			CVE ID: CVE-2024-33067	bulletin.html	
Product: qca					
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-QCA9- 200125/281

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	ources/security bulletin/january -2025- bulletin.html	
Product: qca	19889				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCA9- 200125/282
Product: qcc	2073				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. CVE ID: CVE-2024-45548	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCC2- 200125/283
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCC2- 200125/284
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCC2- 200125/285
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCC2- 200125/286
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-QCC2- 200125/287

4-5

5-6

6-7

3-4

2-3

8-9

9-10

YAY I	n II' I n .	OVICE O	D ' ' ' O OVER ID	D. I	NGURGIR
Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data to WLAN driver. CVE ID: CVE-2024-45542	ources/security bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCC2- 200125/288
Product: qco	2076				
Affected Vers					
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCC2- 200125/289
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCC2- 200125/290
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCC2- 200125/291
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. CVE ID: CVE-2024-45548	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCC2- 200125/292
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCC2- 200125/293

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCHDC ID	
weakness	rublish Date	CV33V3	Description & CVE ID	rattii	NCIIPC ID	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCC2- 200125/294	
Product: qcc	710					
Affected Vers	ion(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCC7- 200125/295	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCC7- 200125/296	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCC7- 200125/297	
Product: qcf	8000					
Affected Vers	ion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCF8- 200125/298	
Product: qcf	8000sfp					

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCF8- 200125/299
Product: qcf	8001				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCF8- 200125/300
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qcr	m4325				
Affected Vers	ion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCM4- 200125/301
			CVE ID: CVE-2024-45553		
Product: qcr	n4490				
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCM4- 200125/302
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCM4- 200125/303

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using it for a process- specific task, issues may arise.	bulletin.html	
			CVE ID: CVE-2024-45553		
Product: qcr	n5430				
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCM5- 200125/304
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCM5- 200125/305
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCM5- 200125/306
Product: qcr	n6490				
Affected Vers					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCM6- 200125/307
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCM6- 200125/308
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element	https://docs.qu alcomm.com/pr oduct/publicres ources/security	H-QUA-QCM6- 200125/309

7-8

9-10

3-4

read 06-Jan-2025 7.3 ID without checking the IE length. CVE ID: CVE-2024-45558 bulletin.html https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-bulletin.html https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin.january -2025-bulletin.html	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcm8550 Affected Version(s): - Buffer Overread				<u> </u>		
Affected Version(s):- Buffer Over- read 06-Jan-2025 06					bulletin.html	
Buffer Over- read 06-Jan-2025 7.5 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 bulletin.html H-QUA-QCM8-20125/310 bulletin.html https://docs.qu alcomm.com/product/publicres ources/security bulletin.january-2025-bulletin.html	Product: qcr	n8550				
Buffer Over- read	Affected Vers	ion(s): -				
Use After Free O6-Jan-2025 6.7 Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055 bulletin/january -2025-bulletin/january -2025-bulletin/january oduct/publicres ources/security bulletin/january -2025-bulletin.html https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin.html https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin.january -2025-bulletin.html https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin.january -2025-bulletin.html https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-bulletin.html https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin.january -2025-bulletin.html		06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCM8- 200125/310
Memory corruption while processing frame command IOCTL calls. H-QUA-QCM8-200125/312		06-Jan-2025	6.7	invoking IOCTL calls to unmap the DMA buffers.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCM8- 200125/311
Use of Out- of-range Pointer Offset O6-Jan-2025 Affected Version(s): - Buffer Over- read O6-Jan-2025 O6-		06-Jan-2025	6.7	processing frame command IOCTL calls.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCM8- 200125/312
Affected Version(s): - Buffer Overread O6-Jan-2025 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries ources/security bulletin/january -2025-bulletin.html	of-range Pointer	06-Jan-2025	6.7	input parameter validation for number of fences is missing for fence frame IOCTL calls,	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCM8- 200125/313
Affected Version(s): - Buffer Overread O6-Jan-2025 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when https://docs.qu alcomm.com/product/publicres ources/security bulletin/january -2025-bulletin.html	Product: acr	15022			buneun.num	
Buffer Over-read O6-Jan-2025 7.5 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur whether the driver parses the per STA profile IE and tries oduct/publicres ources/security bulletin/january -2025-bulletin.html	•					
CVE ID: CVE-2024-45558 bulletin.html	Buffer Over-		7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	alcomm.com/pr oduct/publicres ources/security bulletin/january	H-QUA-QCN5- 200125/314
Product: qcn5024				CVE ID: CVE-2024-45558		
	Product: qcr	15024				
Affected Version(s): -	Affected Vers	ion(s): -				

CVSSv3 Scoring Scale	
* stands for all versions	

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN5- 200125/315
Product: qcr	15052				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN5- 200125/316
Product: qcr	n5122				
Affected Vers					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN5- 200125/317
Product: qcr	15124				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN5- 200125/318
Product: qcr	15152				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCN5- 200125/319

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qcr	15154				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN5- 200125/320
Product: qcr	15164				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCN5- 200125/321
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qcr	16023				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCN6- 200125/322
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qcr	16024				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN6- 200125/323
Product: qcr	16112				
Affected Vers					
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	H-QUA-QCN6-
	, = 0=0				, , , , , , , , , , , , , , , , , , , ,

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/324
Product: qcı	16122				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCN6- 200125/325
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qci					
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCN6- 200125/326
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qcı	16224				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN6- 200125/327
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN6- 200125/328

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558		
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN6- 200125/329
Product: qcr	16274				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN6- 200125/330
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN6- 200125/331
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN6- 200125/332
Product: qcr	16402				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN6- 200125/333

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558		
Product: qcr	16412				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN6- 200125/334
Product: qcr	16422				
Affected Vers					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN6- 200125/335
Product: qcr	16432				
Affected Vers					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN6- 200125/336
Product: qcr	17605				
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN7- 200125/337
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	H-QUA-QCN7- 200125/338

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45542	-2025- bulletin.html	
Product: qcı	17606				
Affected Vers	sion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN7- 200125/339
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN7- 200125/340
Product: qci	19000				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCN9- 200125/341
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qci					
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN9- 200125/342
Product: qci	19022				
Affected Vers					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCN9- 200125/343

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qcr	19024				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN9- 200125/344
Product: qcr	19070				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN9- 200125/345
Product: qcr	20072		CVL 1D. CVL 2021 43330	builetiii.iitiiii	
Affected Vers	sion(s): -		m		l
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN9- 200125/346
Product: qcr	19074				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN9- 200125/347
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every	https://docs.qu alcomm.com/pr oduct/publicres ources/security	H-QUA-QCN9- 200125/348

5-6

6-7

3-4

2-3

8-9

9-10

		valid opcode received from sound model driver.	bulletin/january -2025-	
		CVE ID: CVE-2024-33067	bulletin.html	
19100				
sion(s): -				
06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN9- 200125/349
19160				
sion(s): -				
06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCN9- 200125/350
0274		CVE ID. CVE-2024-43330	Dunetin.ntim	
06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCN9- 200125/351
410				
sion(s): -				
06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS4- 200125/352
06-Jan-2025	6.1	Information disclosure	https://docs.qu	H-QUA-QCS4- 200125/353
	ion(s): - 06-Jan-2025 06-Jan-2025 06-Jan-2025 410 ion(s): -	ion(s): - 06-Jan-2025 7.5 06-Jan-2025 7.5 06-Jan-2025 7.5 410 ion(s): - 06-Jan-2025 7.5	17.5 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. 18.	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 CVE ID: CVE ID: CVE ID: CVE-2024-45558 CVE ID: C

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
Product: qcs	64490				
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS4- 200125/354
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS4- 200125/355
			CVE ID: CVE-2024-45553		
Product: qcs					
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS5- 200125/356
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS5- 200125/357
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS5- 200125/358

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558		
Product: qcs	610				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS6- 200125/359
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCS6- 200125/360
_			CVE ID: CVE-2024-33067	bulletin.html	
Product: qcs					
Affected Vers	sion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QCS6- 200125/361
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS6- 200125/362
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS6- 200125/363
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls,	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	H-QUA-QCS6- 200125/364

Y47 1	D 111 1 D .	OVICE O	D 1 11 0 OVER VD	n . 1	Navina in
Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33041	-2025- bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS6- 200125/365
Product: q	cs7230				
Affected Ve	rsion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS7- 200125/366
Product: q	cs8250				
Affected Ve					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS8- 200125/367
			CVE ID: CVE-2024-45553		
Product: q	cs8550				
Affected Ve	rsion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS8- 200125/368

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS8- 200125/369
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. CVE ID: CVE-2024-33061	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS8- 200125/370
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS8- 200125/371
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS8- 200125/372
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS8- 200125/373
Product: qcs	9100				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QCS9- 200125/374

0-1

5-6

6-7

3-4

2-3

8-9

9-10

Weakı	ness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Produ	ıct: qdı	11000				
Affecte	ed Vers	ion(s): -				
Use After Free		06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QDU1- 200125/375
				CVE ID: CVE-2024-45553		
Produ	ıct: qdı	11010				
Affecte	ed Vers	ion(s): -				
Use Free	After	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QDU1- 200125/376
		1110		CVE ID: CVE-2024-45553		
	ıct: qdı					
Affecte	ed Vers	ion(s): -				
Use Free	After	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QDU1- 200125/377
Produ	ıct: qdı	11210				
		ion(s): -				
Use Free	After	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	H-QUA-QDU1- 200125/378

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while another thread is using it for a process-specific task, issues may arise.	-2025- bulletin.html	
			CVE ID: CVE-2024-45553		
Product: qd	x1010				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QDX1- 200125/379
			CVE ID: CVE-2024-45553		
Product: qd	x1011				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QDX1- 200125/380
			CVE ID: CVE-2024-45553		
Product: qe	p8111				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QEP8- 200125/381
Product: qfv	v7114				
411					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
a v bb v b bcor mg bcare	0 1		_ 0	0 1	1 0	0 0	0 ,	, 0	0 /	, ,

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QFW7- 200125/382
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QFW7- 200125/383
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QFW7- 200125/384
D., J.,	-5404		CVE ID: CVE-2024-33067	bulletin.html	
Product: qfw					
Affected Vers	sion(s): -	I			T
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QFW7- 200125/385
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QFW7- 200125/386
			CVE ID: CVE-2024-45558	bulletin.html	

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		I.C		
06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QFW7- 200125/387
b5165n				
sion(s): -				
06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QRB5- 200125/388
		CVE ID: CVE-2024-45553		
u1032				
sion(s): -				
06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QRU1- 200125/389
		CVE ID: CVE-2024-45553		
u1052				
sion(s): -				
06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QRU1- 200125/390
	b5165n sion(s): - 06-Jan-2025 u1032 sion(s): - 06-Jan-2025	b5165n sion(s): - 06-Jan-2025 7.8 u1032 sion(s): - 06-Jan-2025 7.8	valid opcode received from sound model driver. CVE ID: CVE-2024-33067 b5165n sion(s): - Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 u1032 sion(s): - Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 u1052 sion(s): - Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list. If a map is removed from the global list. If a map is removed from the global list using it for a process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may ir for a process-specific task, issues may arise.	Valid opcode received from sound model driver. CVE ID: CVE-2024-33067

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qr	u1062				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-QRU1- 200125/391
Droduct, ga	m0250		CVE ID. CVE-2024-43333		
Affected Vers					
Affected Vers	Sidil(S): -		Information Plant		
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QSM8- 200125/392
_			CVE ID: CVE-2024-33067	bulletin.html	
Product: qx					
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-QXM8- 200125/393
			CVE ID: CVE-2024-45558	bulletin.html	
Product: rol	botics_rb5				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-ROBO- 200125/394
			CVE ID: CVE-2024-45553		

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sa6	5145p				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA61- 200125/395
			CVE ID: CVE-2024-45555		
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls,	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA61- 200125/396
			CVE ID: CVE-2024-33041	bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA61- 200125/397
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA61- 200125/398
D 1	450		CVE ID: CVE-2024-33067	bulletin.html	
Product: sa6					
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA61- 200125/399

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID)	Patch	l	NCIIF	PC ID
			CVE ID: CVE-	2024-4555	55				
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055		https://doc alcomm.com oduct/publ ources/sec bulletin/jar -2025- bulletin.htm	n/pr icres urity nuary	H-QUA-S. 200125/		
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041		https://doc alcomm.com oduct/publ ources/sec bulletin/jar -2025- bulletin.htm	n/pr icres urity nuary	H-QUA-S. 200125/		
Buffer Over- read	06-Jan-2025	6.1	Information while invo function of driver from valid opcode sound model	ADSP for ever received for driver.	oack odel very rom	https://doc alcomm.com oduct/publ ources/sec bulletin/jar -2025- bulletin.htm	n/pr icres urity nuary	H-QUA-S. 200125/	
Product: sa6	5155								
Affected Vers	sion(s): -								
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.		fied ten, tion. ized into ges, of a tem	https://doc alcomm.cor oduct/publ ources/sec bulletin/jar -2025- bulletin.htm	n/pr icres urity nuary	H-QUA-S. 200125/	
Product: safe	.155n		CVE ID: CVE-	2024-4555	05				
Product: sa6155p Affected Version(s): -									
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system		fied eten, cion. ized into ges, of a	https://doc alcomm.cor oduct/publ ources/sec bulletin/jar -2025- bulletin.htm	n/pr icres urity nuary	H-QUA-S. 200125/	
CVSSv3 Scoring	Scale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			image.		
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA61- 200125/405
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA61- 200125/406
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA61- 200125/407
			GVL ID: GVE-2024-33041	bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA61- 200125/408
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA61- 200125/409
Product: sa7	⁷ 255p				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification.	https://docs.qu alcomm.com/pr oduct/publicres ources/security	H-QUA-SA72- 200125/410

Weakness	Publish Date CVSSv3 Description & CVE ID		Description & CVE ID	Patch	NCIIPC ID		
			This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	bulletin/january -2025- bulletin.html			
			CVE ID: CVE-2024-45555				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA72- 200125/411		
			CVE ID: CVE-2024-45553				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA72- 200125/412		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA72- 200125/413		
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA72- 200125/414		
Product: sa7775p							
Affected Version(s): -							
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA77- 200125/415		

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			security-sensitive images, enabling the booting of a tampered IFS2 system image.	bulletin.html		
			CVE ID: CVE-2024-45555			
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA77- 200125/416	
			CVE ID: CVE-2024-45553			
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA77- 200125/417	
			CVE ID: CVE-2024-45558	bulletin.html		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA77- 200125/418	
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA77- 200125/419	
Product: sa8	R145n			bulletin.html		
Affected Vers						
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA81- 200125/420	

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date CVSSv3 Description & CVE ID		Patch	NCIIPC ID	
			tampered IFS2 system image. CVE ID: CVE-2024-45555		
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA81- 200125/421
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA81- 200125/422
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA81- 200125/423
Duo du at. ao C	01 F O		CVE ID: CVE-2024-33067	bulletin.html	
Product: sa8 Affected Vers					
Affected vers	1011(8)		Memory corruption can		
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA81- 200125/424
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA81- 200125/425
Use of Out- of-range Pointer	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-SA81- 200125/426

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Offset			missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	ources/security bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA81- 200125/427
Product: sa8	 				
Affected Vers					
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA81- 200125/428
			CVE ID: CVE-2024-45555		
Product: sa8	•				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA81- 200125/429
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA81- 200125/430

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA81- 200125/431
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA81- 200125/432
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA81- 200125/433
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA81- 200125/434
			CVE ID: CVE-2024-33067	bulletin.html	
Product: sa8					
Affected Vers	ion(s): -			l	I
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA81- 200125/435
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is	https://docs.qu alcomm.com/pr oduct/publicres ources/security	H-QUA-SA81- 200125/436

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removed from the global list while another thread is using it for a process- specific task, issues may arise.	bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA81- 200125/437
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA81- 200125/438
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA81- 200125/439
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA81- 200125/440
Product: sa8	3255p		0.0000	builetiiiitiiii	
Affected Vers	-				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA82- 200125/441

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA82- 200125/442
			Transient DOS can occur	https://di	
Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA82- 200125/443
			CVE ID: CVE-2024-45558	bulletin.html	
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA82- 200125/444
			CVE ID: CVE-2024-43064	bulletin.html	
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA82- 200125/445
			CVE ID: CVE-2024-23366	bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA82- 200125/446
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA82- 200125/447

CVSSv3 Scoring Scale
* stands for all versions 0-1 2-3 3-4 5-6 6-7 7-8 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sa8	295p				
Affected Vers	ion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA82- 200125/448
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA82- 200125/449
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA82- 200125/450
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA82- 200125/451
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA82- 200125/452
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to	https://docs.qu alcomm.com/pr	H-QUA-SA82- 200125/453

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unmap the DMA buffers.	oduct/publicres	
			CVE ID: CVE-2024-33055	ources/security bulletin/january -2025-	
			Information Disclosure	bulletin.html	
Buffer Over- read	06-Jan-2025	6.6	while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA82- 200125/454
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA82- 200125/455
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA82- 200125/456
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA82- 200125/457
Product: sa8	2520n			bulletin.html	
Affected Vers					
Anicolea vels	1011(3).		Transient DOS can occur		
Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA85- 200125/458
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA85- 200125/459

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33067	bulletin.html	
Product: sa	3540p				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA85- 200125/460
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA85- 200125/461
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA85- 200125/462
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA85- 200125/463
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA85- 200125/464
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API.	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-SA85- 200125/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43063	ources/security bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA85- 200125/466
Product: sa8	3620p			bulletin.html	
Affected Vers					
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA86- 200125/467
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA86- 200125/468
			CVE ID: CVE-2024-45553		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA86- 200125/469
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA86- 200125/470

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558	bulletin.html	
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA86- 200125/471
Product: sa8					
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA86- 200125/472
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA86- 200125/473
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA86- 200125/474
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA86- 200125/475

0-1

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA86- 200125/476
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA86- 200125/477
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA86- 200125/478
Product: sa8	3770p				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA87- 200125/479
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA87- 200125/480
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the	https://docs.qu alcomm.com/pr oduct/publicres ources/security	H-QUA-SA87- 200125/481

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global registers through SMMU. CVE ID: CVE-2024-43064	bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA87- 200125/482
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA87- 200125/483
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA87- 200125/484
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA87- 200125/485
Product: sa8	B775p			bulletin.html	
Affected Vers					
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA87- 200125/486
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-SA87- 200125/487

CVSSv3 Scoring Scale
* stands for all versions

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	ources/security bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45553		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA87- 200125/488
			CVE ID: CVE-2024-43064	bulletin.html	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA87- 200125/489
			CVE ID: CVE-2024-45558	bulletin.html	
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SA87- 200125/490
			CVL 1D. CVL 2024 23300	bulletin.html https://docs.qu	
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA87- 200125/491
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA87- 200125/492
Product: sa9	000p				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten,	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-SA90- 200125/493

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	ources/security bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA90- 200125/494
			CVE ID: CVE-2024-45553		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA90- 200125/495
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA90- 200125/496
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA90- 200125/497
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA90- 200125/498

0-1

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SA90- 200125/499	
Buffer Over- read	06-Jan-2025	CVE ID: CVE-2024-45559 bulletin/january -2025-		https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	H-QUA-SA90- 200125/500	
Product: sc8	180x-aaab					
Affected Vers	ion(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC81- 200125/501	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC81- 200125/502	
Product: sc8	180x-acaf			builetiiiitiiii		
Affected Vers	ion(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC81- 200125/503	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC81- 200125/504	
Product: sc8	180x-ad					

CVSSv3 Scoring Scale
* stands for all versions 3-4 8-9 9-10 0-1 2-3 4-5 5-6 6-7 7-8

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC81- 200125/505	
06-Jan-2025	6-Jan-2025 7.8 INGINIORY COTTUPLION WHEN INCIDENCE AND ARRIVED ARRIV		oduct/publicres ources/security bulletin/january	H-QUA-SC81- 200125/506	
3180xp-aaab					
sion(s): -					
06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC81- 200125/507	
06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SC81- 200125/508	
3180xp-acaf			<u> </u>	1	
sion(s): -					
06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC81- 200125/509	
06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SC81- 200125/510	
	06-Jan-2025 3180xp-aaab sion(s): - 06-Jan-2025 3180xp-acaf sion(s): - 06-Jan-2025	06-Jan-2025 7.8 06-Jan-2025 7.8 06-Jan-2025 7.8 06-Jan-2025 7.8 06-Jan-2025 7.8	10CTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541 Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542 180xp-aaab Sion(s): - Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542 Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542 Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541 Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541 Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541 Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	O6-Jan-2025 7.8 O6-Jan-2025 06-Jan-2025 06-Jan-2025	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC81- 200125/511
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC81- 200125/512
Product: sc8	180x\+sdx55				
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC81- 200125/513
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC81- 200125/514
Product: sc8	280xp-abbb			builetiiiitiiii	
Affected Vers	ion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC82- 200125/515
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC82- 200125/516
Product: sc8	380xp				

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC83- 200125/517
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC83- 200125/518
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC83- 200125/519
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC83- 200125/520
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. CVE ID: CVE-2024-45548	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC83- 200125/521
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. CVE ID: CVE-2024-45550	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SC83- 200125/522
Product: sd8					
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	H-QUA-SD83- 200125/523

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sound model driver.	-2025-	
			CVE ID: CVE-2024-33067	bulletin.html	
Product: sd8	365_5g				l
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067		https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SD86- 200125/524
Product: sdr	n429w				
Affected Vers	sion(s): -				
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SDM4- 200125/525
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SDM4- 200125/526
Product: sdx	x55				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SDX5- 200125/527
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SDX5- 200125/528

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33067	bulletin.html	
Product: sd	x65m				
Affected Ver	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SDX6- 200125/529
Product: sd	_8_gen1_5g				
Affected Ver	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SD_8- 200125/530
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SD_8- 200125/531
Product: sg	4150p				
Affected Ver	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SG41- 200125/532
Product: sg	8275p				
	*				

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): -				
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SG82- 200125/533
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SG82- 200125/534
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SG82- 200125/535
Product: sm	4635				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SM46- 200125/536
			CVE ID: CVE-2024-45553		
Product: sm	6250				
Affected Vers	sion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SM62- 200125/537
Buffer Copy without Checking Size of Input	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data.	https://docs.qu alcomm.com/pr oduct/publicres ources/security	H-QUA-SM62- 200125/538

6-7

7-8

9-10

3-4

('Classic Buffer			the state of the s		
Overflow')			CVE ID: CVE-2024-45541	bulletin/january -2025- bulletin.html	
Product: sm	6650				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SM66- 200125/539
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SM66- 200125/540
Product: sm	7635				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SM76- 200125/541
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SM76- 200125/542
Product: sm	7675				<u> </u>
Affected Vers					

^{*} stands for all versions

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SM76- 200125/543
06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SM76- 200125/544
		CVE ID: CVE-2024-45558	bulletin.html	
ion(s): -				
06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SM76- 200125/545
		CVE ID: CVE-2024-45553		
06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SM76- 200125/546
8550p				
ion(s): -				
06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SM85- 200125/547
	06-Jan-2025 7675p ion(s): - 06-Jan-2025 06-Jan-2025	06-Jan-2025 7.8 06-Jan-2025 7.5 06-Jan-2025 7.8 06-Jan-2025 7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Memory corruption can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Transient DOS can occur when process-specific maps are added to the plobal list. If a map is removed from the global list using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Transient DOS can occur when process-specific maps are added to the plobal list. If a map is removed from the global list using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Transient DOS can occur when process-specific maps are added to the plobal list using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Transient DOS can occur when process-specific maps are added to the plobal list using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45558 Memory corruption can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Delicitin/january -2025-bulletin.html

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific task, issues may arise.		
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SM85- 200125/548
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SM85- 200125/549
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SM85- 200125/550
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SM85- 200125/551
Product: sm	8635			bulletin.html	
Affected Vers					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SM86- 200125/552
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element	https://docs.qu alcomm.com/pr oduct/publicres ources/security	H-QUA-SM86- 200125/553

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID without checking the IE length.	bulletin/january -2025-	
			CVE ID: CVE-2024-45558	bulletin.html	
Product: sm	8635p				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SM86- 200125/554
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SM86- 200125/555
Product: sm	8750				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SM87- 200125/556
Due du et ens	0750		CVE ID: CVE-2024-45558	bulletin.html	
Product: sm Affected Vers					
Antecteu vers	ion(s): -		Tuesdant DOC		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SM87- 200125/557
				i -	

CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9	CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
--	----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakne	SS	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected	l Vers	ion(s): -				
N/A		06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/558
Buffer O read	ver-	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/559
Product	t: sna	pdragon_460_n	nobile			
Affected	Vers	ion(s): -				
Use A Free	After	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/560
Product	t: sna	pdragon_480\+	5g_mob	ile		
Affected		<u> </u>				
Use A Free	After	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/561
Product	t: sna	pdragon_480_5	g_mobile			
Affected		. •				
Use A Free	After	06-Jan-2025	7.8	Memory corruption can occur when process-specific	https://docs.qu alcomm.com/pr	H-QUA-SNAP- 200125/562

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weekness	Dublish Data	CVCC2	Description & CVE ID	Dotah	NCHDC ID
Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
			arise. CVE ID: CVE-2024-45553		
Product: c	napdragon_4_gen	1 mobile			
Affected Ve		_1_11100116	-		
Use Afte Free		7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/563
Product: s	napdragon_4_gen	2 mobile			
Affected Ve		_2_11100110	-		
Use Afte		7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/564
Droduati a	nandragan 662 n	nobilo	CVE ID. CVE-2024-43333		
	napdragon_662_n	nobne			
Affected Ve	ersion(s): -		Momory corruption con		
Use Afte Free	r 06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/565

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakn	iess	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				CVE ID: CVE-2024-45553		
Produ	ct: sna	pdragon_680_4	g_mobile			
Affecte	ed Vers	ion(s): -				
Use Free	After	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/566
				CVE ID: CVE-2024-45553		
Produ	ct: sna	pdragon_685_4	g_mobile			
Affecte	ed Vers	ion(s): -				
Use Free	After	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/567
				CVE ID: CVE-2024-45553		
Produ	ct: sna	pdragon_695_5	g_mobile			
Affecte	ed Vers	ion(s): -				
Use Free	After	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/568
Drodu	ct: enc	pdragon_7c\+_	gen 3 cor			
		ion(s): -	gen_3_cor	npute		
Buffer withou	Copy	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-SNAP- 200125/569

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			data. CVE ID: CVE-2024-45541	ources/security bulletin/january -2025- bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/570
Product: sna	pdragon_7c_co	npute_pl	atform		<u> </u>
Affected Vers	ion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/571
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/572
Product: sna	pdragon_7c_gei	n_2_comp	ute_platform		
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/573
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/574
Product: sna	pdragon_820_a	utomotiv	e		
Affected Vers	ion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten,	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-SNAP- 200125/575

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	ources/security bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45555		
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/576
Product: sna	apdragon_835_n	nohile nc		buneum.num	
Affected Vers		nobne_pc			
Affected vers	51011(5)		T. C 1: 1		
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SNAP- 200125/577
			CVE ID: CVE-2024-33067	bulletin.html	
Product: sna	npdragon_865\+	5g_mob	ile		
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SNAP- 200125/578
			CVE ID: CVE-2024-33067	bulletin.html	
	apdragon_865_5	g_mobile			
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/579

CVSSv3 Scoring Scale	
* stands for all versions	;

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sna	pdragon_870_5	g_mobile			
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/580
Product: sna	pdragon_8\+_g	en_1_mob	pile		
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/581
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/582
Product: sna	pdragon_8\+_g	en_2_mob	oile		
Affected Vers					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/583
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	H-QUA-SNAP- 200125/584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length. CVE ID: CVE-2024-45558	-2025- bulletin.html	
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/585
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/586
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/587
Product: sn	apdragon_8_gen	_1_mobile	2		
Affected Ver	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/588
			CVE ID: CVE-2024-45553		
Product: sn	apdragon_8_gen	_2_mobile	9		<u> </u>
Affected Ver	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/589

CVSSv3 Scoring Scale	
* stands for all versions	;

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/590
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/591
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/592
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/593
Product: sna	npdragon_8_gen	_3_mobile		bulletin.html	
Affected Vers					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/594
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/595

Ī	CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/596
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/597
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/598
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/599
Product: sna	apdragon_ar1_g	en_1			
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/600
			CVE ID: CVE-2024-45553		
	apdragon_ar2_g	en_1			
Affected Vers	sion(s): -				
Use After	06-Jan-2025	7.8	Memory corruption can occur when process-specific	https://docs.qu alcomm.com/pr	H-QUA-SNAP- 200125/601

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	ources/security bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45553		
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/602
Product: sna	apdragon_auto_4	4g_moder	n		
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SNAP- 200125/603
			CVE ID: CVE-2024-33067	bulletin.html	
Product: sna	apdragon_auto_!	5g_moder	n-rf_gen_2		
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/604
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SNAP- 200125/605
			CVE ID: CVE-2024-45558	bulletin.html	
Buffer Over-	06-Jan-2025	6.1	Information disclosure while invoking callback	https://docs.qu alcomm.com/pr	H-QUA-SNAP- 200125/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	ources/security bulletin/january -2025- bulletin.html	
Product: sna	npdragon_w5\+	_gen_1_we	earable		
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/607
			CVE ID: CVE-2024-45553		
Product: sna	apdragon_x35_5	g_modem	-rf		
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/608
			CVE ID: CVE-2024-45553		
	apdragon_x55_5	g_modem	ı-rt		
Affected Vers	sion(s): -		-		
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/609
Product: sna	 apdragon_x65_5	g_modem	ı-rf		
Affected Vers					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-SNAP- 200125/610

4-5

5-6

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	ources/security bulletin/january -2025- bulletin.html	
Droduct, coo	ndvagan v72 F	a modom			
Affected Vers	ion(s):	g_modem	-11		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/611
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/612
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/613
Product: sna	pdragon_x75_5	g modem		bancemmenn	
Affected Vers	• •	00 30111			
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/614
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	H-QUA-SNAP-

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/615
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/616
Product: sna	pdragon_xr2_5	g			
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SNAP- 200125/617
Product: srv	1h				
Affected Vers	ion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SRV1- 200125/618
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SRV1- 200125/619

5-6

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45553		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SRV1- 200125/620
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SRV1- 200125/621
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SRV1- 200125/622
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SRV1- 200125/623
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SRV1- 200125/624
Product: srv	11				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SRV1- 200125/625

CVSSv3 Scoring Scale
* stands for all versions

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			image.		
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SRV1- 200125/626
			CVE ID: CVE-2024-45553		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SRV1- 200125/627
			CVE ID: CVE-2024-43064	bulletin.html	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SRV1- 200125/628
			CVEID. CVE 2021 10000		
Buffer Over-read	06-Jan-2025	06-Jan-2025 5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	H-QUA-SRV1- 200125/629
			CVE ID: CVE-2024-45559	-2025- bulletin.html	
Product: srv	1m				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SRV1- 200125/630

CVSSv3 Scoring Scale
* stands for all versions 0-1 2-3 3-4 5-6 6-7 7-8 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SRV1- 200125/631
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SRV1- 200125/632
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SRV1- 200125/633
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SRV1- 200125/634
Product: ssg	2115p				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SSG2- 200125/635
Use of Out-	06-Jan-2025	6.7	Memory corruption when	https://docs.qu	H-QUA-SSG2-

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVF ID	Patch	NCIIPC ID
	r ublish Date	CV33V3	Description & CVE ID		
of-range Pointer Offset			input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/636
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SSG2- 200125/637
Product: ssg	2125p				
Affected Vers	ion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SSG2- 200125/638
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SSG2- 200125/639
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SSG2- 200125/640
Product: sw	5100				
Affected Vers	ion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SW51- 200125/641

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific task, issues may arise.		
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. CVE ID: CVE-2024-33061	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SW51- 200125/642
Product: sw	5100p				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SW51- 200125/643
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SW51- 200125/644
			CVE ID: CVE-2024-33061	bulletin.html	
Product: sxr					
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SXR1- 200125/645
Use of Out-			Memory corruption when	https://docs.qu	H-QUA-SXR1-
of-range	06-Jan-2025	6.7	input parameter validation	alcomm.com/pr	200125/646

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer Offset		0.00.10	for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	oduct/publicres ources/security bulletin/january -2025- bulletin.html	713212 0 12
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SXR1- 200125/647
Product: sxr	2130				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SXR2- 200125/648
D 1 .	222		CVE ID: CVE-2024-33007	bulletin.html	
Product: sxr	•				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SXR2- 200125/649
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SXR2- 200125/650
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-SXR2- 200125/651

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: sxr	2250p				
Affected Vers	ion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SXR2- 200125/652
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SXR2- 200125/653
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SXR2- 200125/654
Product: sxr	2330p				l
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-SXR2- 200125/655
Product: taly	ynplus				
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-TALY- 200125/656

4-5

5-6

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')				bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-TALY- 200125/657
Product: vid	eo_collaboratio	n vc1	CVE ID: CVE-2024-45555		
		II_VCI			
Affected Vers	ion(s): -		m		ı
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-VIDE- 200125/658
				buneun.numi	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-VIDE- 200125/659
			CVE ID: CVE-2024-33067	bulletin.html	
Product: vid	eo_collaboratio	n_vc3			
Affected Vers	ion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-VIDE- 200125/660
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-VIDE- 200125/661
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-VIDE- 200125/662

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	ources/security bulletin/january -2025- bulletin.html	
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-VIDE- 200125/663
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-VIDE- 200125/664
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-VIDE- 200125/665
Product: vid	eo_collaboratio	n_vc5			
Affected Vers	ion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-VIDE- 200125/666
Product: wc	10335		CVE ID: CVE-2024-45555		
Affected Vers					
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33067		
Product: wc	d9340				
Affected Vers	sion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/668
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/669
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/670
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/671
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/672
Product: wc	d9341				
Affected Vers	sion(s): -				
Stack-based Buffer	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from	https://docs.qu alcomm.com/pr	H-QUA-WCD9- 200125/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow			user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/674
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/675
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/676
Product: wc	d9370				l
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/677
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/678
Buffer Copy without	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from	https://docs.qu alcomm.com/pr	H-QUA-WCD9- 200125/679

CVSSv3 Scoring Scale
* stands for all versions

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			user-space to read board data. CVE ID: CVE-2024-45541	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/680
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/681
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/682
Product: wc	d9375				
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/683
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/684
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WCD9- 200125/685

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using it for a process- specific task, issues may arise. CVE ID: CVE-2024-45553	bulletin.html	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/686
Product: wc	d9378				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/687
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/688
Product: wc	d9380				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/689
Buffer Copy	06-Jan-2025	7.8	Memory corruption when	https://docs.qu	H-QUA-WCD9-

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/690
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/691
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/692
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/693
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. CVE ID: CVE-2024-45548	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/694
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. CVE ID: CVE-2024-45550	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/695
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/696
Use After	06-Jan-2025	6.7	Memory corruption while	https://docs.qu	H-QUA-WCD9-

4-5

5-6

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Free			invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	200125/697
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/698
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/699
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/700
Product: wc	d9385				
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/701
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. CVE ID: CVE-2024-45548	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/702
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	H-QUA-WCD9- 200125/703

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45550	-2025- bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/704
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/705
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/706
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/707
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/708
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/709
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command	https://docs.qu alcomm.com/pr	H-QUA-WCD9- 200125/710

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
	- Homon Butt	0.0070	IOCTL calls.	oduct/publicres	
			CVE ID: CVE-2024-33059	ources/security bulletin/january -2025- bulletin.html	
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/711
Product: wc	d9390				
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/712
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/713
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/714
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/715
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls.	https://docs.qu alcomm.com/pr oduct/publicres	H-QUA-WCD9- 200125/716

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33059	ources/security bulletin/january -2025- bulletin.html	
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/717
Product: wc	d9395				
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/718
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/719
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/720
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/721
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers.	https://docs.qu alcomm.com/pr oduct/publicres ources/security	H-QUA-WCD9- 200125/722

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33055	bulletin/january -2025- bulletin.html	
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCD9- 200125/723
Product: wc	n3620				
Affected Vers	sion(s): -				
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WCN3- 200125/724
			CVE ID: CVE-2024-43064	bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WCN3- 200125/725
			CVE ID: CVE-2024-33067	bulletin.html	
Product: wc	n3660b				
Affected Vers	sion(s): -				
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WCN3- 200125/726
			CVE ID: CVE-2024-43064	bulletin.html	
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WCN3- 200125/727
- aa -			CVE ID: CVE-2024-33061	bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback	https://docs.qu alcomm.com/pr	H-QUA-WCN3- 200125/728

CVSSv3 Scoring Scale	
* stands for all versions	

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
Product: wc	n3680b				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. CVE ID: CVE-2024-33061	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCN3- 200125/729
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCN3- 200125/730
Product: wc	n3950				
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCN3- 200125/731
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCN3- 200125/732
			Transient DOS can occur when the driver parses the	https://docs.qu alcomm.com/pr	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length.	-2025-	
			CVE ID: CVE-2024-45558	bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WCN3- 200125/734
			CVE ID: CVE-2024-33067	bulletin.html	
Product: wc	n3980				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WCN3- 200125/735
			CVE ID: CVE-2024-45558	bulletin.html	
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WCN3- 200125/736
			CVE ID: CVE-2024-33061	bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WCN3- 200125/737
			CVE ID: CVE-2024-33067	bulletin.html	
Product: wc	n3988				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCN3- 200125/738

CVSSv3 Scoring Scale	
* stands for all versions	

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCN3- 200125/739
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WCN3- 200125/740
			CVE ID: CVE-2024-33061	bulletin.html	
Product: wc	n3990				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WCN3- 200125/741
			CVE ID: CVE-2024-33067	bulletin.html	
Product: wc	n6450				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCN6- 200125/742
Buffer Over- read	06-Jan-2025	7.5	CVE ID: CVE-2024-45553 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WCN6- 200125/743

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558		
Product: wc	n6650				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCN6- 200125/744
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCN6- 200125/745
Product: wc	n6740				
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCN6- 200125/746
Product: wc	n6755			Buildinini	
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCN6- 200125/747
Buffer Over-			CVE ID: CVE-2024-45553 Transient DOS can occur	https://docs.qu	H-QUA-WCN6-
read	06-Jan-2025	7.5	when the driver parses the	alcomm.com/pr	200125/748

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			per STA profile IE and tries to access the EXTN element ID without checking the IE length.	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
D J	5060		CVE ID: CVE-2024-45558		
Product: wc					
Affected Vers	sion(s): -		Transient DOS can occur		
Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCN7- 200125/749
Product: wc	n7861				
Affected Vers	sion(s): -				
			Memory corruption can		
Use After Free	06-Jan-2025	7.8	occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCN7- 200125/750
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WCN7- 200125/751
_			CVE ID: CVE-2024-45558	bulletin.html	
Product: wc					
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WCN7- 200125/752

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Descripti	on & CVE	ID	Patch		NCIII	PC ID
Product: wci	n7881								
Affected Vers	ion(s): -								
Use After Free	06-Jan-2025	7.8	Memory cooccur when maps are global list. removed from while anoth using it for specific tast arise.	added to If a ma m the glob her threa or a pro k, issues	the is al list d is ocess-may	https://docs.c alcomm.com/ oduct/publicr ources/securi bulletin/janua -2025- bulletin.html	pr es ity	H-QUA-V 200125/	
Buffer Over- read	06-Jan-2025	7.5	Transient D when the dr per STA pro to access the ID without of length. CVE ID: CVE	river parse file IE and e EXTN ele checking t	tries ment he IE	https://docs.c alcomm.com/ oduct/publicr ources/securi bulletin/janua -2025- bulletin.html	pr es ity	H-QUA-V 200125/	
Product: wsa	a8810								
Affected Vers	ion(s): -								
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory co processing when there clients regist CVE ID: CVE	IPA stati are no a cered.	istics, active	https://docs.o alcomm.com/ oduct/publicr ources/securi bulletin/janua -2025- bulletin.html	pr es ity ary	H-QUA-V 200125/	
Use After Free	06-Jan-2025	7.8	occur when maps are global list.	added to If a ma m the glob her threa or a pro k, issues	the is al list d is ocess-may	https://docs.o alcomm.com/ oduct/publicr ources/securi bulletin/janua -2025- bulletin.html	pr es ty	H-QUA-V 200125/	
Buffer Copy						https://docs.c	111		
without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory co IOCTL call is user-space data. CVE ID: CVE	s invoked to read b	from ooard	alcomm.com/ oduct/publicr ources/securi bulletin/janua -2025- bulletin.html	pr es ty	H-QUA-V 200125/	
Stack-based	06-Jan-2025	7.8	Memory co	rruption	when	https://docs.o	qu	H-QUA-V	VSA8-
				_					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/758
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/759
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/760
Product: ws	a8815				
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/761
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/762
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/763
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	H-QUA-WSA8- 200125/764

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while another thread is using it for a process-specific task, issues may arise.	-2025- bulletin.html	
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/765
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WSA8- 200125/766
			CVE ID: CVE-2024-33067	bulletin.html	
Product: wsa	a8830				
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/767
Overflow') Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/768
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/769
				Duncummen	

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/770
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/771
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. CVE ID: CVE-2024-33061	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/772
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/773
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/774
Product: ws	a8832				
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/775
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	H-QUA-WSA8- 200125/776

CVSSv3 Scoring Scale
* stands for all versions

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while another thread is using it for a process-specific task, issues may arise.	-2025- bulletin.html	
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/777
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/778
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/779
Product: ws	a8835				
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/780
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/781
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WSA8- 200125/782

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')				bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/783
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/784
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. CVE ID: CVE-2024-33061	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/785
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/786
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/787
Product: wsa	a8840				
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WSA8- 200125/788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')				bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/789
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/790
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/791
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/792
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. CVE ID: CVE-2024-45548	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/793
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. CVE ID: CVE-2024-45550	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/794
Buffer Copy without Checking Size of Input	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS	https://docs.qu alcomm.com/pr oduct/publicres ources/security	H-QUA-WSA8- 200125/795

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			encryption and decryption functionality. CVE ID: CVE-2024-45547	bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/796
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/797
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/798
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WSA8- 200125/799
Product: ws:	2004E		CVL 1D. CVL 2021 33011	bulletin.html	
Affected Vers Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/800
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. CVE ID: CVE-2024-45548	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/801
Improper	06-Jan-2025	7.8	Memory corruption occurs	https://docs.qu	H-QUA-WSA8-

CVSSv3 Scoring Scale
* stands for all versions

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls.	alcomm.com/pr oduct/publicres ources/security bulletin/january	200125/802
			CVE ID: CVE-2024-45550	-2025- bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/803
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WSA8- 200125/804
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	bulletin.html https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/805
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/806
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/807
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	H-QUA-WSA8- 200125/808

4-5

5-6

7-8

9-10

3-4

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		length. CVE ID: CVE-2024-45558	-2025- bulletin.html	
06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/809
06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/810
06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls,	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WSA8- 200125/811
00451		CVE ID: CVE-2024-33041	bulletin.html	
ion(s): -	l			
06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	alcomm.com/pr oduct/publicres ources/security bulletin/january	H-QUA-WSA8- 200125/812
		CVL 1D. CVL-2024-21404	bulletin.html	
06-Jan-2025	7.8	occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/813
06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call.	https://docs.qu alcomm.com/pr oduct/publicres ources/security	H-QUA-WSA8- 200125/814
	06-Jan-2025 06-Jan-2025 08845h ion(s): - 06-Jan-2025	06-Jan-2025 6.7 06-Jan-2025 6.7 06-Jan-2025 8.4 06-Jan-2025 7.8	length. CVE ID: CVE-2024-45558 Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059 Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055 Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041 Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464 Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Memory corruption while processing FIPS encryption or decryption validation v	length.

CVSSv3 Scoring Scale
* stands for all versions

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/815
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. CVE ID: CVE-2024-45550	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/816
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/817
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/818
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/819
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/820
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls,	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	H-QUA-WSA8- 200125/821

0-1

4-5

5-6

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33041	bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055 https://docs alcomm.com oduct/public ources/secu bulletin/jant-2025-bulletin.htm		H-QUA-WSA8- 200125/822
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	H-QUA-WSA8- 200125/823
			Operating System		
Vendor: For	tinet				
Product: for	tios				
Affected Vers	sion(s): From (inc	cluding) 7.	0.0 Up to (excluding) 7.0.17		
Authenticati on Bypass Using an Alternate Path or Channel	14-Jan-2025	9.8	An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] affecting FortiOS version 7.0.0 through 7.0.16 and FortiProxy version 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12 allows a remote attacker to gain super-admin privileges via crafted requests to Node.js websocket module.	https://fortigua rd.fortinet.com/ psirt/FG-IR-24- 535	O-FOR-FORT- 200125/824
			CVE ID: CVE-2024-55591		
Vendor: Goo					
Product: and					
Affected Vers	sion(s): -				
N/A	08-Jan-2025	7.8	In DevmemIntMapPages of devicemem_server.c, there is a possible physical page uaf due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges	N/A	O-GOO-ANDR- 200125/825

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation.		
			CVE ID: CVE-2023-35685		
Vendor: Hua	wei				
Product: em	ui				
Affected Vers	ion(s): 12.0.0				
Improper Privilege Management	08-Jan-2025	7.8	Vulnerability of improper permission control in the window management module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/826
			CVE ID: CVE-2024-56447		
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect availability.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/827
injection j			CVE ID: CVE-2024-56448		
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/828
			CVE ID: CVE-2024-56449		
N/A	08-Jan-2025	6.5	Vulnerability of improper authentication in the ANS system service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/829
			CVE ID: CVE-2023-52955		
Improper Limitation of a Pathname to a	08-Jan-2025	6.2	Path traversal vulnerability in the Medialibrary module Impact: Successful exploitation of this	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/830

0-1

5-6

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			vulnerability will affect integrity and confidentiality. CVE ID: CVE-2023-52953		
N/A	08-Jan-2025	5.5	Vulnerability of native APIs not being implemented in the NFC service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. CVE ID: CVE-2024-56442	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/831
N/A	08-Jan-2025	4.4	Vulnerability of improper permission control in the Gallery module Impact: Successful exploitation of this vulnerability may affect availability. CVE ID: CVE-2023-52954	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/832
Concurrent Execution using Shared Resource with Improper Synchroniza tion ('Race Condition')	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56441	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/833
	sion(s): 13.0.0				
Improper Privilege Management	08-Jan-2025	7.8	Vulnerability of improper permission control in the window management module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56447	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/834
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/835

0-1

4-5

5-6

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability.		
			CVE ID: CVE-2024-56448		
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56449	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/836
N/A	08-Jan-2025	6.5	Vulnerability of improper authentication in the ANS system service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. CVE ID: CVE-2023-52955	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/837
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2025	6.2	Path traversal vulnerability in the Medialibrary module Impact: Successful exploitation of this vulnerability will affect integrity and confidentiality. CVE ID: CVE-2023-52953	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/838
N/A	08-Jan-2025	6.2	Permission control vulnerability in the Connectivity module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. CVE ID: CVE-2024-56440	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/839
N/A	08-Jan-2025	5.5	Vulnerability of native APIs not being implemented in the NFC service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. CVE ID: CVE-2024-56442	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/840

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Jan-2025	4.4	Vulnerability of improper permission control in the Gallery module Impact: Successful exploitation of this vulnerability may affect availability. CVE ID: CVE-2023-52954	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/841
Concurrent Execution using Shared Resource with Improper Synchroniza tion ('Race	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56441	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/842
Condition')			CVE ID: CVE-2024-30441		
Affected Vers	sion(s): 14.0.0				
Improper Privilege Management	08-Jan-2025	7.8	Vulnerability of improper permission control in the window management module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/843
			CVE ID: CVE-2024-56447		
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect availability.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/844
, ,			CVE ID: CVE-2024-56448		
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56449	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/845
Buffer Copy without Checking	08-Jan-2025	6.3	Buffer overflow vulnerability in the component driver module	https://consum er.huawei.com/ en/support/bull	O-HUA-EMUI- 200125/846

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Size of Input ('Classic Buffer Overflow')			Impact: Successful exploitation of this vulnerability may affect availability.	etin/2025/1/		
			CVE ID: CVE-2024-56450			
N/A	08-Jan-2025	6.2	Permission control vulnerability in the Connectivity module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/847	
			CVE ID: CVE-2024-56440			
N/A	08-Jan-2025	6	Vulnerability of improper memory address protection in the HUKS module Impact: Successful exploitation of this vulnerability may affect availability.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/848	
			CVE ID: CVE-2024-56438			
Operation on a Resource after Expiration or Release	08-Jan-2025	4.4	UAF vulnerability in the device node access module Impact: Successful exploitation of this vulnerability may cause service exceptions of the device.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/849	
			CVE ID: CVE-2024-56434			
Concurrent Execution using Shared Resource with Improper Synchroniza	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-EMUI- 200125/850	
tion ('Race Condition')			CVE ID: CVE-2024-56441			
Product: har	rmonyos					
Affected Vers	ion(s): 2.0.0					
Improper Privilege Management	08-Jan-2025	7.8	Vulnerability of improper permission control in the window management module Impact: Successful	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/851	

CVSSv3 Scoring Scale
* stands for all versions

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may affect service confidentiality.		
			CVE ID: CVE-2024-56447		
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect availability.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/852
			CVE ID: CVE-2024-56448		
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/853
			CVE ID: CVE-2024-56449		
N/A	08-Jan-2025	6.5	Vulnerability of improper authentication in the ANS system service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/854
			CVE ID: CVE-2023-52955		
Improper Limitation of a Pathname to a Restricted Directory ('Path	08-Jan-2025	6.2	Path traversal vulnerability in the Medialibrary module Impact: Successful exploitation of this vulnerability will affect integrity and confidentiality.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/855
Traversal')			CVE ID: CVE-2023-52953		
N/A	08-Jan-2025	5.5	Vulnerability of native APIs not being implemented in the NFC service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/856

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-56442		
N/A	08-Jan-2025	4.4	Vulnerability of improper permission control in the Gallery module Impact: Successful exploitation of this vulnerability may affect availability. CVE ID: CVE-2023-52954	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/857
Concurrent Execution using Shared Resource with Improper Synchroniza tion ('Race Condition')	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56441	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/858
Affected Vers	sion(s): 2.1.0				
Improper Privilege Management	08-Jan-2025	7.8	Vulnerability of improper permission control in the window management module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56447	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/859
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect availability. CVE ID: CVE-2024-56448	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/860
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56449	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/861
N/A	08-Jan-2025	6.5	Vulnerability of improper	https://consum	O-HUA-HARM-

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication in the ANS system service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	er.huawei.com/ en/support/bull etin/2025/1/	200125/862
			CVE ID: CVE-2023-52955		
Improper Limitation of a Pathname to a Restricted Directory ('Path	08-Jan-2025	6.2	Path traversal vulnerability in the Medialibrary module Impact: Successful exploitation of this vulnerability will affect integrity and confidentiality.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/863
Traversal')			CVE ID: CVE-2023-52953		
N/A	08-Jan-2025	5.5	Vulnerability of native APIs not being implemented in the NFC service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/864
			CVE ID: CVE-2024-56442		
N/A	08-Jan-2025	4.4	Vulnerability of improper permission control in the Gallery module Impact: Successful exploitation of this vulnerability may affect availability.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/865
			CVE ID: CVE-2023-52954		
Concurrent Execution using Shared Resource with Improper Synchroniza tion ('Race	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56441	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/866
Condition') Affected Vers	ion(s)·300				
Improper	1011(3). 3.0.0		Vulnerability of improper	https://consum	
Privilege Management	08-Jan-2025	7.8	permission control in the window management	er.huawei.com/ en/support/bull	O-HUA-HARM- 200125/867

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	etin/2025/1/	
			CVE ID: CVE-2024-56447		
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect availability.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/868
			CVE ID: CVE-2024-56448		
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/869
			CVE ID: CVE-2024-56449		
N/A	08-Jan-2025	6.5	Vulnerability of improper authentication in the ANS system service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/870
			CVE ID: CVE-2023-52955		
Improper Limitation of a Pathname to a Restricted Directory ('Path	08-Jan-2025	6.2	Path traversal vulnerability in the Medialibrary module Impact: Successful exploitation of this vulnerability will affect integrity and confidentiality.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/871
Traversal')			CVE ID: CVE-2023-52953		
N/A	08-Jan-2025	6.2	Permission control vulnerability in the Connectivity module Impact: Successful exploitation of this vulnerability may cause features to perform	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/872

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			abnormally.		
			CVE ID: CVE-2024-56440		
N/A	08-Jan-2025	5.5	Vulnerability of native APIs not being implemented in the NFC service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/873
			CVE ID: CVE-2024-56442		
N/A	08-Jan-2025	4.4	Vulnerability of improper permission control in the Gallery module Impact: Successful exploitation of this vulnerability may affect availability.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/874
			CVE ID: CVE-2023-52954		
Concurrent Execution using Shared Resource with Improper Synchroniza tion ('Race	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56441	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/875
Condition')			CVEID: CVE 2021 30111		
Affected Vers	sion(s): 3.1.0				
Improper Privilege Management	08-Jan-2025	7.8	Vulnerability of improper permission control in the window management module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/876
			CVE ID: CVE-2024-56447		
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect availability.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/877

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-56448		
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/878
			CVE ID: CVE-2024-56449		
N/A	08-Jan-2025	6.5	Vulnerability of improper authentication in the ANS system service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/879
			CVE ID: CVE-2023-52955		
N/A	08-Jan-2025	6.2	Permission control vulnerability in the Connectivity module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/880
			CVE ID: CVE-2024-56440		
N/A	08-Jan-2025	6	Vulnerability of improper memory address protection in the HUKS module Impact: Successful exploitation of this vulnerability may affect availability.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/881
			CVE ID: CVE-2024-56438		
N/A	08-Jan-2025	5.5	Vulnerability of native APIs not being implemented in the NFC service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/882
			CVE ID: CVE-2024-56442		
N/A	08-Jan-2025	4.4	Vulnerability of improper	https://consum	O-HUA-HARM-

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permission control in the Gallery module Impact: Successful exploitation of this vulnerability may affect availability. CVE ID: CVE-2023-52954	er.huawei.com/ en/support/bull etin/2025/1/	200125/883
Concurrent Execution using Shared Resource with Improper Synchroniza tion ('Race Condition')	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56441	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/884
Affected Vers	sion(s): 4.0.0				l
Improper Privilege Management	08-Jan-2025	7.8	Vulnerability of improper permission control in the window management module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/885
			CVE ID: CVE-2024-56447		
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect availability.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/886
, · · · · ,			CVE ID: CVE-2024-56448		
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/887
Buffer Copy without Checking Size of Input	08-Jan-2025	6.3	Buffer overflow vulnerability in the component driver module Impact: Successful	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/888

0-1

4-5

5-6

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			exploitation of this vulnerability may affect availability.		
			CVE ID: CVE-2024-56450		
N/A	08-Jan-2025	6.2	Permission control vulnerability in the Connectivity module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. CVE ID: CVE-2024-56440	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/889
N/A	08-Jan-2025	6	Vulnerability of improper memory address protection in the HUKS module Impact: Successful exploitation of this vulnerability may affect availability. CVE ID: CVE-2024-56438	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/890
Operation on a Resource after Expiration or Release	08-Jan-2025	4.4	UAF vulnerability in the device node access module Impact: Successful exploitation of this vulnerability may cause service exceptions of the device. CVE ID: CVE-2024-56434	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/891
Concurrent Execution using Shared Resource with Improper Synchroniza tion ('Race Condition')	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56441	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/892
Affected Vers	sion(s): 4.2.0				
Improper Privilege Management	08-Jan-2025	7.8	Vulnerability of improper permission control in the window management module Impact: Successful exploitation of this vulnerability may affect	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/893

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service confidentiality.		
			CVE ID: CVE-2024-56447		
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect availability. CVE ID: CVE-2024-56448	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/894
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56449	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/895
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Jan-2025	6.3	Buffer overflow vulnerability in the component driver module Impact: Successful exploitation of this vulnerability may affect availability. CVE ID: CVE-2024-56450	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/896
N/A	08-Jan-2025	6.2	Permission control vulnerability in the Connectivity module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. CVE ID: CVE-2024-56440	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/897
N/A	08-Jan-2025	6	Vulnerability of improper memory address protection in the HUKS module Impact: Successful exploitation of this vulnerability may affect availability. CVE ID: CVE-2024-56438	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/898
Operation on a	08-Jan-2025	4.4	UAF vulnerability in the device node access module	https://consum er.huawei.com/	O-HUA-HARM- 200125/899

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource after Expiration or Release			Impact: Successful exploitation of this vulnerability may cause service exceptions of the device.	en/support/bull etin/2025/1/	
			CVE ID: CVE-2024-56434		
Concurrent Execution using Shared Resource with Improper Synchroniza tion ('Race Condition')	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56441	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/900
Affected Vers	sion(s): 5.0.0				
Protection Mechanism Failure	08-Jan-2025	7.5	Access control vulnerability in the identity authentication module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56439	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/901
N/A	08-Jan-2025	7.5	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56444	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/902
Integer Overflow to Buffer Overflow	08-Jan-2025	7.3	Integer overflow vulnerability during glTF model loading in the 3D engine module Impact: Successful exploitation of this vulnerability may affect availability. CVE ID: CVE-2024-56451	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/903
Buffer Copy without Checking Size of Input ('Classic	08-Jan-2025	6.8	Vulnerability of input parameters not being verified during glTF model loading in the 3D engine module	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/904

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Impact: Successful exploitation of this vulnerability may affect availability.		
			CVE ID: CVE-2024-56456		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Jan-2025	6.8	Vulnerability of input parameters not being verified during glTF model loading in the 3D engine module Impact: Successful exploitation of this vulnerability may affect availability.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/905
			CVE ID: CVE-2024-56453		
Improper Input Validation	08-Jan-2025	6.2	Startup control vulnerability in the ability module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/906
			CVE ID: CVE-2024-54121		
Exposure of Sensitive Information to an Unauthorize d Actor	08-Jan-2025	6.2	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56443	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/907
Exposure of Sensitive Information to an Unauthorize d Actor	08-Jan-2025	6.2	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56435	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/908
Improper Input Validation	08-Jan-2025	5.7	Vulnerability of input parameters not being verified in the widget framework module Impact: Successful exploitation of this	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/909

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may affect availability.		
			CVE ID: CVE-2024-56437		
N/A	08-Jan-2025	5.5	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID: CVE-2024-56436	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/910
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Jan-2025	5.5	Vulnerability of input parameters not being verified during glTF model loading in the 3D engine module Impact: Successful exploitation of this vulnerability may affect availability. CVE ID: CVE-2024-56455	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/911
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Jan-2025	5.5	Vulnerability of input parameters not being verified during glTF model loading in the 3D engine module Impact: Successful exploitation of this vulnerability may affect availability.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/912
			CVE ID: CVE-2024-56454		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Jan-2025	5.5	Vulnerability of input parameters not being verified during glTF model loading in the 3D engine module Impact: Successful exploitation of this vulnerability may affect availability. CVE ID: CVE-2024-56452	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/913
Improper Authenticati on	08-Jan-2025	4.3	Instruction authentication bypass vulnerability in the Findnetwork module Impact: Successful exploitation of this	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/914

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may cause features to perform abnormally. CVE ID: CVE-2024-56445		
Concurrent Execution using Shared Resource with Improper Synchroniza tion ('Race Condition')	08-Jan-2025	4.1	Race condition vulnerability in the distributed notification module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. CVE ID: CVE-2024-54120	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/915
Use of Uninitialized Variable	08-Jan-2025	4	Vulnerability of variables not being initialized in the notification module Impact: Successful exploitation of this vulnerability may affect availability.	https://consum er.huawei.com/ en/support/bull etin/2025/1/	O-HUA-HARM- 200125/916
** 1 **			CVE ID: CVE-2024-56446		
Vendor: Lini					
Product: line		1 1: 2	4.0.222		
Affected vers	sion(s): * Up to (e	xciuaing)	4.9.333		T
Allocation of Resources Without Limits or Throttling	02-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: s5p_cec: limit msg.len to CEC_MAX_MSG_SIZE I expect that the hardware will have limited this to 16, but just in case it hasn't, check for this corner case. CVE ID: CVE-2022-49035	https://git.kern el.org/stable/c/ 1609231f86760 c1f6a429de791 3dd795b9faa08 c, https://git.kern el.org/stable/c/ 2654e785bd4aa 2439cdffbe7dc1 ea30a0eddbfe4, https://git.kern el.org/stable/c/ 4a449430ecfb1 99b99ba58af63 c467eb53500b3 9	O-LIN-LINU- 200125/917
Affected Vers	sion(s): * Up to (e	xcluding)			
			In the Linux kernel, the following vulnerability has	https://git.kern el.org/stable/c/	O-LIN-LINU-

CVSSv3 Scoring Scale
* stands for all versions

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MIPS: Loongson64: DTS: Really fix PCIe port nodes	bd056dc2eb823	
			for ls7a Fix the dtc warnings:	https://git.kern el.org/stable/c/ 4fbd66d8254ce dfd1218393f39	
			arch/mips/boot/dts/loongs on/ls7a-pch.dtsi:68.16- 416.5: Warning (interrupt_provider): /bus@10000000/pci@1a0 00000: '#interrupt-cells' found, but node is not an interrupt provider	d83b6c07a0191 7, https://git.kern el.org/stable/c/ 5a2eaa3ad2b80 3c7ea442c6db7 379466ee73c02	
			arch/mips/boot/dts/loongs on/ls7a-pch.dtsi:68.16- 416.5: Warning (interrupt_provider): /bus@10000000/pci@1a0 00000: '#interrupt-cells' found, but node is not an interrupt provider		
			arch/mips/boot/dts/loongs on/loongson64g_4core_ls7a .dtb: Warning (interrupt_map): Failed prerequisite 'interrupt_provider'		
			And a runtime warning introduced in commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"):		
			WARNING: CPU: 0 PID: 1 at drivers/of/base.c:106 of_bus_n_addr_cells+0x9c/0 xe0 Missing '#address-cells' in		
			/bus@10000000/pci@1a0 00000/pci_bridge@9,0		
			The fix is similar to commit d89a415ff8d5 ("MIPS: Loongson64: DTS: Fix PCIe port nodes for ls7a"), which		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has fixed the issue for ls2k (despite its subject mentions ls7a).		
			CVE ID: CVE-2024-56785		
Affected Vers	sion(s): * Up to (e	excluding)	5.15.174		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: soc: imx8m: Probe the SoC driver as platform driver With driver_async_probe=* on kernel command line, the following trace is produced because on i.MX8M Plus hardware because the soc-imx8m.c driver calls of_clk_get_by_name() which returns - EPROBE_DEFER because the clock driver is not yet probed. This was not detected during regular testing without driver_async_probe. Convert the SoC code to platform driver and instantiate a platform device in its current device_initicall() to probe the platform driver. Rework .soc_revision callback to always return valid error code and return SoC revision via parameter. This way, if anything in the .soc_revision callback return -EPROBE_DEFER, it gets propagated to .probe and the .probe will get retried later. "	https://git.kern el.org/stable/c/ 2129f6faa5dfe8 c6b87aad11720 bf75edd77d3e4, https://git.kern el.org/stable/c/ 997a3c04d7fa3 d1d385c146913 50d096fada648 c, https://git.kern el.org/stable/c/ 9cc832d37799d bea950c4c8a34 721b02b8b5a8ff	O-LIN-LINU- 200125/919

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WARNING: CPU: 1 PID: 1 at		
			drivers/soc/imx/soc-		
			imx8m.c:115		
			imx8mm_soc_revision+0xdc		
			/0x180		
			CPU: 1 UID: 0 PID: 1 Comm:		
			swapper/0 Not tainted		
			6.11.0-next-20240924-		
			00002-g2062bb554dea		
			#603		
			Hardware name: DH electronics i.MX8M Plus		
			electronics i.MX8M Plus DHCOM Premium		
			Developer Kit (3) (DT)		
			pstate: 20000005 (nzCv daif		
			-PAN -UAO -TCO -DIT -SSBS		
			BTYPE=)		
			pc :		
			imx8mm_soc_revision+0xdc		
			/0x180		
			lr :		
			imx8mm_soc_revision+0xd		
			0/0x180		
			sp : ffff8000821fbcc0		
			x29: ffff8000821fbce0 x28:		
			0000000000000000 x27:		
			ffff800081810120		
			x26: ffff8000818a9970 x25:		
			00000000000000006 x24: 0000000000824311		
			x23: ffff8000817f42c8 x22:		
			ffff0000df8be210 x21:		
			ffffffffffffffffb		
			x20: ffff800082780000 x19:		
			0000000000000001 x18:		
			fffffffffffff		
			x17: ffff800081fff418 x16:		
			ffff8000823e1000 x15:		
			ffff0000c03b65e8		
			x14: ffff0000c00051b0 x13:		
			ffff800082790000 x12:		
			000000000000000000000000000000000000000		
			x11: ffff80008278ffff x10:		
			ffff80008209d3a6 x9 :		
			ffff80008062e95c x8: ffff8000821fb9a0 x7:		
			x8 : mi8000821fb9a0 x7 : 000000000000000000000000000000000		
			000000000000000 x8 :		
			x5 : ffff0000df8c03d8 x4 :		
			00000000000000000 x3 :		
			000000000000000000000000000000000000000		
			x2 : 00000000000000000 x1		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			: ffffffffffffffb x0 : ffffffffffffffffb Call trace: imx8mm_soc_revision+0xdc /0x180 imx8_soc_init+0xb0/0x1e0 do_one_initcall+0x94/0x1a 8 kernel_init_freeable+0x240 /0x2a8 kernel_init+0x28/0x140 ret_from_fork+0x10/0x20[end trace 000000000000000000000000000000000000		
Affacted Vers	sion(s): * Up to (e	veluding)	CVE ID: CVE-2024-56787		
Missing Release of Memory after Effective Lifetime	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix nfs4_openowner leak when concurrent nfsd4_open occur The action force umount(umount -f) will attempt to kill all rpc_task even umount operation may ultimately fail if some files remain open. Consequently, if an action attempts to open a file, it can potentially send two rpc_task to nfs server. NFS CLIENT thread1 thread2 open("file") nfs4_do_opennfs4_do_opennfs4_open_and_get_state	https://git.kern el.org/stable/c/ 0ab0a3ad24e97 0e894abcac58f8 5c332d1726749 , https://git.kern el.org/stable/c/ 2d505a801e574 28057563762f6 7a5a62009b260 0, https://git.kern el.org/stable/c/ 37dfc81266d3a 32294524bfadd 3396614f8633e e	O-LIN-LINU- 200125/920

0-1

4-5

5-6

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_nfs4_proc_open nfs4_run_open_task /* rpc_task1 */ rpc_run_task		
			rpc_wait_for_completion_tas		
			umount -		
			nfs_umount_begin		
			rpc_killall_tasks		
			rpc_signal_task rpc_task1 been wakeup and return -512 _nfs4_do_open // while loop		
			nfs4_run_open_task /* rpc_task2 */ rpc_run_task		
			rpc_wait_for_completion_tas		
			While processing an open request, nfsd will first attempt to find or allocate an nfs4_openowner. If it finds an nfs4_openowner that is		
			not marked as NFS4_OO_CONFIRMED, this nfs4_openowner will released. Since		
			two rpc_task can attempt to open the same file simultaneously from the client to server, and because two instances of nfsd can run		
			concurrently, this situation can lead to lots of memory leak. Additionally, when we echo 0 to /proc/fs/nfsd/threads, warning will be		
			triggered.		

CVSSv3 Scoring Scale
* stands for all versions

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NFS SERVER nfsd1 nfsd2 echo 0 > /proc/fs/nfsd/threads		
			nfsd4_open nfsd4_process_open1		
			find_or_alloc_open_stateow ner // alloc oo1, stateid1 nfsd4_open		
			nfsd4_process_open1		
			find_or_alloc_open_stateow ner // find oo1, without NFS4_OO_CONFIRMED		
			release_openowner		
			unhash_openowner_locked		
			list_del_init(&oo- >oo_perclient)		
			alloc_stateowner // alloc oo2		
			nfsd4_process_open2 init_open_stateid // associate oo1 // with stateid1, stateid1 LEAK!!! nfs4_get_vfs_file // alloc nfsd_file1 and nfsd_file_mark1 // all LEAK!!!		
			nfsd4_process_open2 		
			write_threads		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nfsd_destroy_serv		
			nfsd_shutdown_net		
			nfs4_state_shutdown_net		
			nfs4_state_destroy_net		
			destroy_client		
			destroy_client		
			won't find oo1!!!		
			nfsd_shutdown_generic		
			nfsd_file_cache_shutdown		
			kmem_cache_destroy		
			for nfsd_file_slab		
			and nfsd_file_mark_slab		
			// bark since nfsd_file1		
			// and nfsd_file_mark1		
			// still alive		
			=======================================		
			=======================================		
			====== BUG nfsd_file (Not tainted):		
			Objects remaining in		
			nfsd_file on _kmem_cache_shutdown()		
			0		
			Slab 0xffd4000004438a80 objects=34 used=1		
			fp=0xff11000110e2ad28		
			flags=0x17ffffc0000240(wo		
			rkingset head node=0 zone =2 lastcpupid=0x1fffff)		
			CPU: 4 UID: 0 PID: 757		
			Comm: sh Not tainted 6.12.0-rc6+ #19		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Missing '#size-cells' in /pci@f2000000/mac-io@c/escc@13000 6, WARNING: CPU: 0 PID: 0 at drivers/of/base.c:133 of_bus_n_size_cells+0x98/0 a26005eecc272 691284c2cd33ff aa0b35ce53b32	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
In the Linux kernel, the following vulnerability has been resolved: powerpc/prom_init: Fixup missing powermac #size-cells On some powermacs 'escc' nodes are missing `#size-cells' properties, which is deprecated and now triggers a warning at boot since commit 045b14ca5c36 ("of: WARN 0b94d838018fb on deprecated #address-cells/#size-cells dandling"). N/A O8-Jan-2025 5.5 Missing '#size-cells' in /pci@f2000000/mac-io@c/escc@13000 WARNING: CPU: 0 PID: 0 at drivers/of/base.c:133 of_bus_n_size_cells+0x98/0 x108 In the Linux kernel, the following vulnerability has been resolved: Don some powermacs 'escc' nodes are missing `#size-cells and https://git.kern el.org/stable/c/2045b14ca5c36 ("of: WARN 0b94d838018fb 0a824e0cd3149 034928c99fb1b nandling"). N/A O8-Jan-2025 O-Jan-2025 Missing '#size-cells' in /pci@f2000000/mac-io@c/escc@13000 dacdoosecc272 (bocomosofic properties, which is deprecated and now triggers a warning at boot since commit el.org/stable/c/ 296a109fa7711 0ba5267fe0e90 a26005eecc272 (bocomosofic properties, which is deprecated and now triggers a warning at boot since commit el.org/stable/c/ 296a109fa7711 0ba5267fe0e90 a26005eecc272 (bocomosofic properties, which is deprecated and now triggers a warning at boot since commit el.org/stable/c/ 296a109fa7711 0ba5267fe0e90 a26005eecc272 (bocomosofic properties, which is deprecated and now triggers a warning at boot since commit el.org/stable/c/ 296a109fa7711 0ba5267fe0e90 a26005eecc272 (bocomosofic properties, which is deprecated and now triggers a warning at boot since commit el.org/stable/c/ 296a109fa7711 0ba5267fe0e90 a26005eecc272 (bocomosofic properties, which is deprecated and hot triggers a warning at boot since commit el.org/stable/c/ 296a109fa7711 0ba5267fe0e90 a26005eecc272 (bocomosofic properties, which is deprecated and hot triggers a warning at boot since commit el.org/stable/c/ 296a109fa7711 0ba5267fe0e90 a26005eecc272 (bocomosofic properties, which is deprecated and hot triggers a warning at boot since commit el.org/stable/c/ 296a109fa7				Standard PC (i440FX + PIIX, 1996), BIOS 1.16.1-2.fc37 04/01/2014 Call Trace: <task> dumtruncated</task>		
				CVE ID: CVE-2024-56779		
Hardware name: PowerMac3,1 7400 0xc0209 PowerMac Call Trace: of_bus_n_size_cells+0x98/0 x108 (unreliable) of_bus_default_count_cells+ 0x40/0x60	N/A	08-Jan-2025	5.5	following vulnerability has been resolved: powerpc/prom_init: Fixup missing powermac #size-cells On some powermacs `escc` nodes are missing `#size-cells` properties, which is deprecated and now triggers a warning at boot since commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"). For example: Missing '#size-cells' in /pci@f2000000/mac-io@c/escc@13000 WARNING: CPU: 0 PID: 0 at drivers/of/base.c:133 of_bus_n_size_cells+0x98/0 x108 Hardware name: PowerMac3,1 7400 0xc0209 PowerMac Call Trace: of_bus_n_size_cells+0x98/0 x108 (unreliable) of_bus_default_count_cells+	el.org/stable/c/ 0b94d838018fb 0a824e0cd3149 034928c99fb1b 7, https://git.kern el.org/stable/c/ 296a109fa7711 0ba5267fe0e90 a26005eecc272 6, https://git.kern el.org/stable/c/ 691284c2cd33ff	O-LIN-LINU- 200125/921

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	Description & CVE ID 1c of_address_to_resource+0 x5c/0x228 pmz_init_port+0x5c/0x2ec pmz_probe.isra.0+0x144/0x 1e4 pmz_console_init+0x10/0x4 8 console_init+0xcc/0x138 start_kernel+0x5c4/0x694 As powermacs boot via prom_init it's possible to add the missing properties to the device tree during boot, avoiding the warning. Note that `escc-legacy` nodes are also missing `#size-cells` properties, but they are skipped by the macio driver, so leave them alone. Depends-on: 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling")	Patch	NCIIPC ID
			CVE ID: CVE-2024-56781		
Affected Vers	sion(s): * Up to (e	xcluding)			
Missing Release of Memory after Effective Lifetime	08-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix handling of plane refcount [Why] The mechanism to backup and restore plane states doesn't maintain refcount, which can cause issues if the refcount of the plane changes in between backup and	https://git.kern el.org/stable/c/ 27227a234c148 7cb7a684615f0 749c455218833 a, https://git.kern el.org/stable/c/ 8cb2f6793845f1 35b28361ba8e9 6901cae3e5790	O-LIN-LINU- 200125/922

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restore operations, such as memory leaks if the refcount was supposed to go down, or double frees / invalid memory accesses if the refcount was supposed to go up.		
			[How] Cache and re-apply current refcount when restoring plane states.		
ACC 1 XI	(-) * II - 1 - (-	-1 -1: -1	CVE ID: CVE-2024-56775		
Out-of- bounds Write	on(s): * Up to (e	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Adding array index check to prevent memory corruption [Why & How] Array indices out of bound caused memory corruption. Adding checks to ensure that array index stays in bound. CVE ID: CVE-2024-56784	https://git.kern el.org/stable/c/ 2c437d9a0b496 168e1a1defd17 b531f0a526dbe 9, https://git.kern el.org/stable/c/ dff526dc3e27f5 484f5ba11471b 9fbbe681467f2	O-LIN-LINU- 200125/923
NULL Pointer Dereference	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: ACPI: x86: Add adev NULL check to acpi_quirk_skip_serdev_enu meration() acpi_dev_hid_match() does not check for adev == NULL, dereferencing it unconditional. Add a check for adev being NULL before calling acpi_dev_hid_match(). At the moment acpi_quirk_skip_serdev_enu	https://git.kern el.org/stable/c/ 4a49194f587a6 2d972b602e3e1 a2c3cfe6567966 , https://git.kern el.org/stable/c/ e173bce05f703 2a8b4964cfef82 a4b7668f5f3af	O-LIN-LINU- 200125/924

0-1

4-5

5-6

6-7

8-9

9-10

7-8

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): * Up to (e	eveluding	meration() is never called with a controller_parent without an ACPI companion, but better safe than sorry. CVE ID: CVE-2024-56782		
Use After Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix use-after-free when COWing tree bock and tracing is enabled When a COWing a tree block, at btrfs_cow_block(), and we have the tracepoint trace_btrfs_cow_block() enabled and preemption is also enabled (CONFIG_PREEMPT=y), we can trigger a use-after-free in the COWed extent buffer while inside the tracepoint code. This is because in some paths that call btrfs_cow_block(), such as btrfs_search_slot(), we are holding the last reference on the extent buffer @buf so btrfs_force_cow_block() drops the last reference on the @buf extent buffer when it calls free_extent_buffer_stale(buf), which schedules the release of the extent buffer with RCU. This means that if we are on a kernel with preemption, the current task may be preempted before calling trace_btrfs_cow_block() and the extent buffer already released by the time trace_btrfs_cow_block() is called, resulting in a use-	https://git.kern el.org/stable/c/ 44f52bbe96dfdb e4aca3818a253 4520082a07040 , https://git.kern el.org/stable/c/ c3a403d8ce36f5 a809a492581de 5ad17843e4701	O-LIN-LINU- 200125/925

0-1

4-5

5-6

6-7

8-9

9-10

7-8

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			after-free. Fix this by moving the trace_btrfs_cow_block() from btrfs_cow_block() to btrfs_force_cow_block() before the COWed extent buffer is freed. This also has a side effect of invoking the tracepoint in the tree defrag code, at defrag.c:btrfs_realloc_node(), since btrfs_force_cow_block() is called there, but this is fine and it was actually missing there. CVE ID: CVE-2024-56759		
Improper Resource Shutdown or Release	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btusb: mediatek: add intf release flow when usb disconnect MediaTek claim an special usb intr interface for ISO data transmission. The interface need to be released before unregistering hci device when usb disconnect. Removing BT usb dongle without properly releasing the interface may cause Kernel panic while unregister hci device. CVE ID: CVE-2024-56757	https://git.kern el.org/stable/c/ 489304e67087a bddc2666c5af0 159cb95afdcf59, https://git.kern el.org/stable/c/ cc569d791ab2a 0de74f76e4705 15d25d24c9b84 b	0-LIN-LINU- 200125/926
Affected Vers	sion(s): * Up to (e	xcluding)	6.6.66		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: put bpf_link's program when link is safe to be deallocated	https://git.kern el.org/stable/c/ 2fcb921c2799c4 9ac5e365cf4110 f94a64ae4885, https://git.kern el.org/stable/c/	0-LIN-LINU- 200125/927

CVSSv3 Scoring Scale
* stands for all versions

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	In general, BPF link's underlying BPF program should be considered to be reachable through attach hook -> link -> prog chain, and, pessimistically, we have to assume that as long as link's memory is not safe to free, attach hook's code might hold a pointer to BPF program and use it. As such, it's not (generally) correct to put link's program early before waiting for RCU GPs to go through. More eager bpf_prog_put() that we currently do is mostly correct due to BPF program's release code doing similar RCU GP waiting, but as will be shown in the following patches, BPF program can be nonsleepable (and, thus, reliant on only "classic" RCU GP), while BPF link's attach hook can have sleepable semantics and needs to be protected by RCU Tasks Trace, and for such cases BPF link has to go through RCU Tasks Trace + "classic" RCU GPs before being deallocated. And so, if we put BPF program early, we might free BPF link, leading to use-after-free situation	Fatch 5fe23c57abadfd 46a7a66e81f35 36e4757252a0b , https://git.kern el.org/stable/c/f 44ec8733a8469 143fde1984b5e 6931b2e2f6f3f	NCIIPC ID
			= =		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			one extra RCU GP, but that seems completely acceptable. Alternatively, we'd need more elaborate ways to determine BPF hook, BPF link, and BPF program lifetimes, and how they relate to each other, which seems like an unnecessary complication. Note, for most BPF links we still will perform eager bpf_prog_put() and link dealloc, so for those BPF links there are no observable changes whatsoever. Only BPF links that use deferred dealloc might notice slightly delayed freeing of BPF programs. Also, to reduce code and logic duplication, extract program put + link dealloc logic into bpf_link_dealloc() helper. CVE ID: CVE-2024-56786		
Affected Vers	sion(s): 6.1				
Allocation of Resources Without Limits or Throttling	02-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: s5p_cec: limit msg.len to CEC_MAX_MSG_SIZE I expect that the hardware will have limited this to 16, but just in case it hasn't, check for this corner case. CVE ID: CVE-2022-49035	https://git.kern el.org/stable/c/ 1609231f86760 c1f6a429de791 3dd795b9faa08 c, https://git.kern el.org/stable/c/ 2654e785bd4aa 2439cdffbe7dc1 ea30a0eddbfe4, https://git.kern el.org/stable/c/ 4a449430ecfb1 99b99ba58af63 c467eb53500b3 9	O-LIN-LINU- 200125/928
Affected Vers	sion(s): 6.13				L

CVSSv3 Scoring Scale
* stands for all versions 2-3 3-4 4-5 5-6 6-7 7-8 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries/vas: Add close() callback in vas_vm_ops struct The mapping VMA address is saved in VAS window struct when the paste address is mapped. This VMA address is used during migration to unmap the paste address if the window is active. The paste address mapping will be removed when the window is closed or with the munmap(). But the VMA address in the VAS window is not updated with munmap() which is causing invalid access during migration. The KASAN report shows: [16386.254991] BUG: KASAN: slab-use-after-free in reconfig_close_windows+0x 1a0/0x4e8 [16386.255043] Read of size 8 at addr c00000014a819670 by task drmgr/696928 [16386.255096] CPU: 29 UID: 0 PID: 696928 Comm: drmgr Kdump: loaded Tainted: G B 6.11.0-rc5-nxgzip #2 [16386.255128] Tainted: [B]=BAD_PAGE [16386.255148] Hardware name: IBM,9080-HEX Power11 (architected) 0x820200 0xf000007 of:IBM,FW1110.00 (NH1110_016) hv:phyp pSeries	https://git.kern el.org/stable/c/ 05aa156e156ef 3168e7ab8a687 21945196495c1 7, https://git.kern el.org/stable/c/ 6d9cd27105459 f169993a4c5f21 6499a946dbf34, https://git.kern el.org/stable/c/ 8b2282b508452 1254a2cd9742a 3f4e1d5b77f843	O-LIN-LINU- 200125/929

0-1

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[16386.255181] Call Trace: [16386.255202] [c00000016b297660] [c000000018ad0ac] dump_stack_lvl+0x84/0xe8 (unreliable) [16386.255246] [c00000016b297690] [c000000006e8a90] print_report+0x19c/0x764 [16386.255285] [c00000016b297760] [c0000000006e9490] kasan_report+0x128/0x1f8 [16386.255309] [c00000016b297880] [c00000016b297880] [c00000006eb5c8] _asan_load8+0xac/0xe0 [16386.255326] [c00000016b2978a0] [c000000016b2978a0] [c0000000013f898] reconfig_close_windows+0x 1a0/0x4e8 [16386.255343] [c00000016b297990] [c00000000140e58] vas_migration_handler+0x3 a4/0x3fc [16386.255368] [c00000016b297a90] [c0000000000128848] pseries_migrate_partition+0		
			x4c/0x4c4 [16386.256136] Allocated by task 696554 on cpu 31 at 16377.277618s: [16386.256149] kasan_save_stack+0x34/0x 68 [16386.256163] kasan_save_track+0x34/0x 80 [16386.256175] kasan_save_alloc_info+0x58 /0x74 [16386.256196]kasan_slab_alloc+0xb8/0x dc [16386.256209] kmem_cache_alloc_noprof+		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x200/0x3d0 [16386.256225] vm_area_alloc+0x44/0x150 [16386.256245] mmap_region+0x214/0x10 c4 [16386.256265] do_mmap+0x5fc/0x750 [16386.256277] vm_mmap_pgoff+0x14c/0x 24c [16386.256292] ksys_mmap_pgoff+0x20c/0 x348 [16386.256303] sys_mmap+0xd0/0x160		
			[16386.256350] Freed by task 0 on cpu 31 at 16386.204848s: [16386.256363] kasan_save_stack+0x34/0x 68 [16386.256374] kasan_save_track+0x34/0x 80 [16386.256384] kasan_save_free_info+0x64/0x10c [16386.256396]kasan_slab_free+0x120/0 x204 [16386.256415] kmem_cache_free+0x128/0 x450		
			[16386.256428] vm_area_free_rcu_cb+0xa8/ 0xd8 [16386.256441] rcu_do_batch+0x2c8/0xcf0 [16386.256458] rcu_core+0x378/0x3c4 [16386.256473] handle_softirqs+0x20c/0x6 0c [16386.256495] do_softirq_own_stack+0x6c /0x88 [16386.256509] do_softirq_own_stack+0x58 /0x88		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[16386.256521] _irq_exit_rcu+0x1a4/0x20c [16386.256533] irq_exit+0x20/0x38 [16386.256544] interrupt_async_exit_prepar e.constprop.0+0x18/0x2c		
			[16386.256717] Last potentially related work creation: [16386.256729] kasan_save_stack+0x34/0x 68 [16386.256741]kasan_record_aux_stack+0 xcc/0x12c [16386.256753]call_rcu_common.constpro p.0+0x94/0xd04 [16386.256766] vm_area_free+0x28/0x3c [16386.256778] remove_vma+0xf4/0x114 [16386.256797] do_vmi_align_munmap.cons tprop.0+0x684/0x870 [16386.256811]		
			_vm_munmap+0xe0/0x1f8 [16386.256821] sys_munmap+0x54/0x6c [16386.256830] system_call_exception+0x1a 0/0x4a0 [16386.256841] system_call_vectored_comm on+0x15c/0x2ec		
			[16386.256868] The buggy address belongs to the object at c00000014a819670 which belongs to the cache vm_area_struct of size 168 [16386.256887] The buggy address is located 0 bytes inside of freed 168-byte region [c00000014a819670,		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			c00000014a819718) [16386.256915] The buggy address belongs to the physical page: [16386.256928] page: refcount:1 mapcount:0 mapping:000000000000000000000000000000000000		
Use After Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ublk: detach gendisk from ublk device if add_disk() fails Inside ublk_abort_requests(), gendisk is grabbed for aborting all inflight requests. And ublk_abort_requests() is called when exiting the uring context or handling timeout. If add_disk() fails, the gendisk may have been freed when calling ublk_abort_requests(), so use-after-free can be caused when getting disk's reference in ublk_abort_requests(). Fixes the bug by detaching gendisk from ublk device if add_disk() fails.	https://git.kern el.org/stable/c/ 75cd4005da549 2129917a4a4ee 45e8166055610 4, https://git.kern el.org/stable/c/ 7d680f2f76a341 7fdfc3946da747 1e81464f7b41	O-LIN-LINU- 200125/930

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-56764		
Use After Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix use-after-free when COWing tree bock and tracing is enabled When a COWing a tree block, at btrfs_cow_block(), and we have the tracepoint trace_btrfs_cow_block() enabled and preemption is also enabled (CONFIG_PREEMPT=y), we can trigger a use-after-free in the COWed extent buffer while inside the tracepoint code. This is because in some paths that call btrfs_cow_block(), such as btrfs_search_slot(), we are holding the last reference on the extent buffer @buf so btrfs_force_cow_block() drops the last reference on the @buf extent buffer when it calls free_extent_buffer_stale(buf), which schedules the release of the extent buffer with RCU. This means that if we are on a kernel with preemption, the current task may be preempted before calling trace_btrfs_cow_block() and the extent buffer already released by the time trace_btrfs_cow_block() is called, resulting in a use-after-free. Fix this by moving the trace_btrfs_cow_block() to btrfs_force_cow_block() to btrfs_force_cow_block() to btrfs_force_cow_block()	https://git.kern el.org/stable/c/ 44f52bbe96dfdb e4aca3818a253 4520082a07040 , https://git.kern el.org/stable/c/ c3a403d8ce36f5 a809a492581de 5ad17843e4701	O-LIN-LINU- 200125/931

CVSSv3 Scoring Scale
* stands for all versions 0-1 2-3 3-4 5-6 6-7 7-8 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before the COWed extent buffer is freed. This also has a side effect of invoking the tracepoint in the tree defrag code, at defrag.c:btrfs_realloc_node(), since btrfs_force_cow_block() is called there, but this is fine and it was actually missing there. CVE ID: CVE-2024-56759		
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free. CVE ID: CVE-2024-56766	https://git.kern el.org/stable/c/ 6ea15205d7e2b 811fbbdf79783f 686f58abfb4b7, https://git.kern el.org/stable/c/ d2f090ea57f8d6 587e09d4066f7 40a8617767b3d , https://git.kern el.org/stable/c/ d8e4771f99c04 00a1873235704 b28bb803c83d1 7	O-LIN-LINU- 200125/932
Use of Uninitialized Resource	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: dvb-frontends: dib3000mb: fix uninit-value in dib3000_write_reg Syzbot reports [1] an uninitialized value issue found by KMSAN in dib3000_read_reg(). Local u8 rb[2] is used in i2c_transfer() as a read buffer; in case that call fails, the buffer may end up with some undefined values.	https://git.kern el.org/stable/c/ 1d6de21f00293 d819b5ca6dbe7 5ff1f3b6392140, https://git.kern el.org/stable/c/ 2dd59fe0e19e1 ab95525997808 2b62e5751924c 7, https://git.kern el.org/stable/c/ 3876e3a1c31a5 8a352c6bf5d2a 90e3304445a63 7	O-LIN-LINU- 200125/933

0-1

4-5

5-6

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Since no elaborate error handling is expected in dib3000_write_reg(), simply zero out rb buffer to mitigate the problem.		
			[1] Syzkaller report dvb-usb: bulk message failed: -22 (6/0) ====================================		
			dib3000mb_attach+0x2d8/ 0x3c0 drivers/media/dvb- frontends/dib3000mb.c:75 8		
			dibusb_dib3000mb_fronten d_attach+0x155/0x2f0 drivers/media/usb/dvb- usb/dibusb-mb.c:31		
			dvb_usb_adapter_frontend_i nit+0xed/0x9a0 drivers/media/usb/dvb- usb/dvb-usb-dvb.c:290 dvb_usb_adapter_init drivers/media/usb/dvb- usb/dvb-usb-init.c:90 [inline] dvb_usb_init drivers/media/usb/dvb- usb/dvb-usb-init.c:186 [inline]		
			dvb_usb_device_init+0x25a 8/0x3760 drivers/media/usb/dvb- usb/dvb-usb-init.c:310 dibusb_probe+0x46/0x250 drivers/media/usb/dvb- usb/dibusb-mb.c:110		
			 Local variable rb created at:		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dib3000_read_reg+0x86/0x 4e0 drivers/media/dvb- frontends/dib3000mb.c:54		
			dib3000mb_attach+0x123/ 0x3c0 drivers/media/dvb- frontends/dib3000mb.c:75 8		
			CVE ID: CVE-2024-56769		
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix bpf_get_smp_processor_id() on !CONFIG_SMP On x86-64 calling bpf_get_smp_processor_id() in a kernel with CONFIG_SMP disabled can trigger the following bug, as pcpu_hot is unavailable: [8.471774] BUG: unable to handle page fault for address: 00000000936a290c [8.471849] #PF: supervisor read access in kernel mode	https://git.kern el.org/stable/c/ 23579010cf0a1 2476e96a5f1acd f78a9c5843657, https://git.kern el.org/stable/c/f 4ab7d74247b01 50547cf909b3f6 f24ee85183df	O-LIN-LINU- 200125/934
			[8.471881] #PF: error_code(0x0000) - not-present page Fix by inlining a return 0 in the !CONFIG_SMP case. CVE ID: CVE-2024-56768		
			In the Linux kernel, the	https://git.kern	
NULL Pointer Dereference	06-Jan-2025	5.5	following vulnerability has been resolved: dmaengine: at_xdmac: avoid null_prt_deref in at_xdmac_prep_dma_memse t	el.org/stable/c/ 54376d8d2659 6f98ed7432a78 8314bb9154bf3 e3, https://git.kern el.org/stable/c/ c43ec96e8d343	O-LIN-LINU- 200125/935

CVSSv3 Scoring Scale
* stands for all versions 3-4 0-1 2-3 4-5 5-6 7-8 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The at_xdmac_memset_create_d esc may return NULL, which will lead to a null pointer dereference. For example, the len input is error, or the atchan->free_descs_list is empty and memory is exhausted. Therefore, add check to avoid this. CVE ID: CVE-2024-56767	99bd9dab2f2dc 316b904892133 f, https://git.kern el.org/stable/c/ e658f1c133b85 4b2ae79914730 1d82dddb8f316 2	
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: tracing: Prevent bad count for tracing_cpumask_write If a large count is provided, it will trigger a warning in bitmap_parse_user. Also check zero for it. CVE ID: CVE-2024-56763	https://git.kern el.org/stable/c/ 03041e474a6a8 f1bfd4b96b164 bb3165c48fa1a 3, https://git.kern el.org/stable/c/ 1cca920af19df5 dd91254e5ff35e 68e911683706, https://git.kern el.org/stable/c/ 3d15f4c244955 8ffe83b4dba306 14ef1cd6937c3	O-LIN-LINU- 200125/936
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: x86/fred: Clear WFE in missing-ENDBRANCH #CPs An indirect branch instruction sets the CPU indirect branch tracker (IBT) into WAIT_FOR_ENDBRANCH (WFE) state and WFE stays asserted across the instruction boundary. When the decoder finds an inappropriate instruction while WFE is set ENDBR, the CPU raises a #CP fault.	https://git.kern el.org/stable/c/ b939f108e86b7 6119428a6fa4e 92491e09ac786 7, https://git.kern el.org/stable/c/ dc81e556f2a01 7d681251ace21 bf06c126d5a19 2	O-LIN-LINU- 200125/937

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			For the "kernel IBT no ENDBR" selftest where #CPs are deliberately triggered, the WFE state of the interrupted context needs to be cleared to let execution continue. Otherwise when the CPU resumes from the instruction that just caused the previous #CP, another missing-ENDBRANCH #CP is raised and the CPU enters a dead loop.		
			This is not a problem with IDT because it doesn't preserve WFE and IRET doesn't set WFE. But FRED provides space on the entry stack (in an expanded CS area) to save and restore the WFE state, thus the WFE state is no longer clobbered, so software must clear it.		
			Clear WFE to avoid dead looping in ibt_clear_fred_wfe() and the !ibt_fatal code path when execution is allowed to continue. Clobbering WFE in any other circumstance is a security-relevant bug.		
			[dhansen: changelog rewording] CVE ID: CVE-2024-56761		
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: PCI/MSI: Handle lack of irqdomain gracefully	https://git.kern el.org/stable/c/ a60b990798eb1 7433d02837882 80422b1bd94b1 8, https://git.kern	O-LIN-LINU- 200125/938

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Alexandre observed a warning emitted from pci_msi_setup_msi_irqs() on a RISCV platform which does not provide PCI/MSI support: WARNING: CPU: 1 PID: 1 at drivers/pci/msi/msi.h:121 pci_msi_setup_msi_irqs+0x2 c/0x32	el.org/stable/c/ aed157301c659 a48f5564cc456 8cf0e5c8831af0, https://git.kern el.org/stable/c/ b1f7476e07b93 d65a1a3643dcb 4a7bed80d4328 d	
			pci_enable_msix_range+0x 30c/0x596 pci_msi_setup_msi_irqs+0x2		
			c/0x32 pci_alloc_irq_vectors_affinit y+0xb8/0xe2		
			RISCV uses hierarchical interrupt domains and correctly does not implement the legacy fallback. The warning triggers from the legacy fallback stub.		
			That warning is bogus as the PCI/MSI layer knows whether a PCI/MSI parent domain is associated with the device or not. There is a check for MSI-X, which has a legacy assumption. But that legacy fallback assumption is only valid when legacy support is enabled, but otherwise the check should simply return -ENOTSUPP.		
			Loongarch tripped over the same problem and blindly enabled legacy support without implementing the legacy fallbacks. There are weak implementations which return an error, so the problem was papered		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			over. Correct pci_msi_domain_supports() to evaluate the legacy mode and add the missing supported check into the MSI enable path to complete it. CVE ID: CVE-2024-56760 In the Linux kernel, the		
NULL Pointer Dereference	06-Jan-2025	5.5	btrfs: check folio mapping after unlock in relocate_one_folio() When we call btrfs_read_folio() to bring a folio uptodate, we unlock the folio. The result of that is that a different thread can modify the mapping (like remove it with invalidate) before we call folio_lock(). This results in an invalid page and we need to try again. In particular, if we are relocating concurrently with aborting a transaction, this can result in a crash like the following: BUG: kernel NULL pointer dereference, address: 00000000000000000000000000000000000	https://git.kern el.org/stable/c/ 3e74859ee35ed c33a022c3f397 1df066ea0ca6b9 , https://git.kern el.org/stable/c/ d508e56270389 b3a16f5b3cf247 f4eb1bbad1578	O-LIN-LINU- 200125/939

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ed+0x20/0xb0		
			RSP:		
			0018:ffffc900516a7be8		
			EFLAGS: 00010246		
			RAX: ffffea009e851d08		
			RBX: ffffea009e0b1880		
			RCX: 000000000000000000		
			RDX: 000000000000000000		
			RSI: ffffc900516a7b90 RDI:		
			ffffea009e0b1880		
			RBP: 0000000003573000		
			R08: 00000000000000001		
			R09: ffff88c07fd2f3f0		
			R10: 00000000000000000000000000000000000		
			R11: 0000194754b575be		
			R12: 0000000003572000 R13: 000000003572fff		
			R13: 0000000003572fff R14: 000000000100cca		
			R15: 0000000005582fff		
			FS:		
			000000000000000000000000000000000000000		
			GS:ffff88c07fd00000(0000)		
			knlGS:00000000000000000		
			CS: 0010 DS: 0000 ES:		
			0000 CR0:		
			0000000080050033		
			CR2: 000000000000000000		
			CR3: 000000407d00f002		
			CR4: 00000000007706f0		
			DR0: 00000000000000000		
			DR1: 00000000000000000		
			DR2: 00000000000000000		
			DR3: 00000000000000000		
			DR6: 00000000fffe0ff0		
			DR7: 0000000000000400		
			PKRU: 55555554		
			Call Trace:		
			<task></task>		
			?die+0x78/0xc0		
			?		
			page_fault_oops+0x2a8/0x3		
			a0		
			?		
			_switch_to+0x133/0x530		
			•		
			wq_worker_running+0xa/0 x40		
			X4U 7		
			•		
			exc_page_fault+0x63/0x130		
			: asm_exc_page_fault+0x22/0		
			x30		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? set_page_extent_mapped+0 x20/0xb0		
			relocate_file_extent_cluster+ 0x1a7/0x940		
			relocate_data_extent+0xaf/ 0x120		
			relocate_block_group+0x20f /0x480		
			btrfs_relocate_block_group+ 0x152/0x320		
			btrfs_relocate_chunk+0x3d/ 0x120		
			btrfs_reclaim_bgs_work+0x 2ae/0x4e0		
			process_scheduled_works+ 0x184/0x370		
			worker_thread+0xc6/0x3e0		
			t blk_add_timer+0xb0/0xb0 kthread+0xae/0xe0		
			flush_tlb_kernel_range+0x9 0/0x90 ret_from_fork+0x2f/0x40		
			? flush_tlb_kernel_range+0x9 0/0x90		
			ret_from_fork_asm+0x11/0 x20 		
			This occurs because cleanup_one_transaction() calls		
			destroy_delalloc_inodes() which calls		
			invalidate_inode_pages2() which		
			takes the folio_lock before		
			setting mapping to NULL. We fail to check		
			this, and subsequently call		

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			set_extent_mapping(), which assumes that mapping != NULL (in fact it asserts that in debug mode)		
			Note that the "fixes" patch here is not the one that introduced the race (the very first iteration of this code from 2009) but a more recent change that made this particular crash happen in practice.		
			CVE ID: CVE-2024-56758		
			In the Linux kernel, the following vulnerability has been resolved: net/sched: netem: account		
N/A	08-Jan-2025	5.5	net/sched: netem: account for backlog updates from child qdisc In general, 'qlen' of any classful qdisc should keep track of the number of packets that the qdisc itself and all of its children holds. In case of netem, 'qlen' only accounts for the packets in its internal tfifo. When netem is used with a child qdisc, the child qdisc can use 'qdisc_tree_reduce_backlog' to inform its parent, netem, about created or dropped SKBs. This function updates 'qlen' and the backlog statistics of netem, but netem does not account for changes made by a child qdisc. 'qlen' then indicates the wrong number of packets in the tfifo. If a child qdisc creates new SKBs during enqueue and	https://git.kern el.org/stable/c/ 10df49cfca73df bbdb6c4150d85 9f7e8926ae427, https://git.kern el.org/stable/c/ 216509dda290f 6db92c816dd54 b83c1df9da9e7 6, https://git.kern el.org/stable/c/ 356078a5c55ec 8d2061fcc009fb 8599f5b0527f9	O-LIN-LINU- 200125/940

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			about this, netem's 'qlen' value is increased. When netem dequeues the newly created SKBs from the child, the 'qlen' in netem is not updated. If 'qlen' reaches the configured sch->limit, the enqueue function stops working, even though the tfifo is not full.		
			Reproduce the bug: Ensure that the sender machine has GSO enabled. Configure netem as root qdisc and tbf as its child on the outgoing interface of the machine as follows: \$ tc qdisc add dev <oif> root handle 1: netem delay 100ms limit 100 \$ tc qdisc add dev <oif> parent 1:0 tbf rate 50Mbit burst 1542 latency 50ms</oif></oif>		
			Send bulk TCP traffic out via this interface, e.g., by running an iPerf3 client on the machine. Check the qdisc statistics: \$ tc -s qdisc show dev <oif></oif>		
			Statistics after 10s of iPerf3 TCP test before the fix (note that netem's backlog > limit, netem stopped accepting packets): qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 2767766 bytes 1848 pkt (dropped 652, overlimits 0 requeues 0) backlog 4294528236b 1155p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms		
			Sent 2767766 bytes 1848 pkt (dropped 327,		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			-		
			overlimits 7601 requeues 0)		
			backlog 0b 0p requeues 0		
			backing ob op requeues o		
			Statistics after the fix:		
			qdisc netem 1: root refcnt 2		
			limit 1000 delay 100ms		
			Sent 37766372 bytes		
			24974 pkt (dropped 9,		
			overlimits 0 requeues 0)		
			backlog 0b 0p requeues 0		
			qdisc tbf 10: parent 1:1 rate		
			50Mbit burst 1537b lat		
			50ms		
			Sent 37766372 bytes		
			24974 pkt (dropped 327,		
			overlimits 96017 requeues 0)		
			backlog 0b 0p requeues 0		
			sacinos os op requeues o		
			tbf segments the GSO SKBs		
			(tbf_segment) and updates		
			the netem's 'qlen'.		
			The interface fully stops		
			transferring packets and		
			"locks". In this case,		
			the child qdisc and tfifo are		
			empty, but 'qlen' indicates		
			the tfifo is at		
			its limit and no more		
			packets are accepted.		
			This patch adds a counter		
			for the entries in the tfifo.		
			Netem's 'qlen' is		
			only decreased when a		
			packet is returned by its		
			dequeue function, and not		
			during enqueuing into the		
			child qdisc. External		
			updates to 'qlen' are thus		
			accounted for and only the		
			behavior of the backlog		
			statistics changes. As		
			in other qdiscs, 'qlen' then		
			keeps track of how many		
			packets are held in		
			netem and all of its children. As before, sch->limit		
			As before, sch->limit remains as the		
			maximum number of		
			packets in the tfifo. The		
	<u> </u>		packets in the tillo. The		<u> </u>

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			same applies to netem's backlog statistics. CVE ID: CVE-2024-56770		
NULL Pointer Dereference	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: add a sanity check for btrfs root in btrfs_search_slot() Syzbot reports a null-ptr-deref in btrfs_search_slot(). The reproducer is using rescue=ibadroots, and the extent tree root is corrupted thus the extent tree is NULL. When scrub tries to search the extent tree to gather the needed extent info, btrfs_search_slot() doesn't check if the target root is NULL or not, resulting the null-ptr-deref. Add sanity check for btrfs root before using it in btrfs_search_slot(). CVE ID: CVE-2024-56774	https://git.kern el.org/stable/c/ 3ed51857a50f5 30ac7a1482e06 9dfbd1298558d 4, https://git.kern el.org/stable/c/ 757171d1369b3 b47f36932d40a 05a0715496dca b, https://git.kern el.org/stable/c/ 93992c3d9629b 02dccf6849238 559d5c24f2dece	O-LIN-LINU- 200125/941
Reachable Assertion	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_socket: remove WARN_ON_ONCE on maximum cgroup level cgroup maximum depth is INT_MAX by default, there is a cgroup toggle to restrict this maximum depth to a more reasonable value not to harm performance. Remove unnecessary	https://git.kern el.org/stable/c/ 2f9bec0a749eb6 46b384fde0c7b 7c24687b2ffae, https://git.kern el.org/stable/c/ 7064a6daa4a70 0a298fe3aee11d ea296bfe59fc4, https://git.kern el.org/stable/c/ b7529880cb961 d515642ce63f9 d7570869bbbdc 3	O-LIN-LINU- 200125/942

0-1

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WARN_ON_ONCE which is reachable from userspace.		
			CVE ID: CVE-2024-56783		
			In the Linux kernel, the following vulnerability has been resolved:		
			quota: flush quota_release_work upon quota writeback		
			One of the paths quota writeback is called from is:		
			freeze_super() sync_filesystem() ext4_sync_fs()		
			dquot_writeback_dquots()	https://git.kern el.org/stable/c/	
N/A	08-Jan-2025	5.5	Since we currently don't always flush the quota_release_work queue in this path, we can end up with the following race:	3e6ff207cd5bd9 24ad94cd1a7c6 33bcdac0ba1cb, https://git.kern el.org/stable/c/ 6f3821acd7c31 4314599924808	0-LIN-LINU- 200125/943
			1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state:	7de5fb4b48cf26 , https://git.kern el.org/stable/c/ 8ea87e3479225 8825d290f4dc5 216276e91cb22 4	- ,
		ext4_journal_check_start+0x 28/0x110 [ext4] (unreliable)			
			_ext4_journal_start_sb+0x6 4/0x1c0 [ext4]		

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ext4_release_dquot+0x90/0 x1d0 [ext4]		
			quota_release_workfn+0x43 c/0x4d0		
			Which is the following line:		
			WARN_ON(sb- >s_writers.frozen == SB_FREEZE_COMPLETE);		
			Which ultimately results in generic/390 failing due to dmesg noise. This was detected on powerpc machine 15 cores.		
			To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze.		
			CVE ID: CVE-2024-56780		
Affected Vers	sion(s): From (inc	cluding) 2.	6.19 Up to (excluding) 6.1.12	23	
			In the Linux kernel, the following vulnerability has been resolved:	https://git.kern	
			media: dvb-frontends: dib3000mb: fix uninit-value in dib3000_write_reg	el.org/stable/c/ 1d6de21f00293 d819b5ca6dbe7 5ff1f3b6392140,	
Use of Uninitialized Resource	06-Jan-2025	5.5	Syzbot reports [1] an uninitialized value issue found by KMSAN in dib3000_read_reg().	https://git.kern el.org/stable/c/ 2dd59fe0e19e1 ab95525997808 2b62e5751924c	O-LIN-LINU- 200125/944
			Local u8 rb[2] is used in i2c_transfer() as a read buffer; in case that call fails, the buffer may end up with some undefined values.	7, https://git.kern el.org/stable/c/ 3876e3a1c31a5 8a352c6bf5d2a 90e3304445a63	
			Since no elaborate error handling is expected in dib3000_write_reg(),	,	

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			simply zero out rb buffer to mitigate the problem.		
			[1] Syzkaller report dvb-usb: bulk message failed: -22 (6/0)		
			=======================================		
			BUG: KMSAN: uninit-value in dib3000mb_attach+0x2d8/ 0x3c0 drivers/media/dvb-frontends/dib3000mb.c:75		
			dib3000mb_attach+0x2d8/ 0x3c0 drivers/media/dvb- frontends/dib3000mb.c:75 8		
			dibusb_dib3000mb_fronten d_attach+0x155/0x2f0 drivers/media/usb/dvb- usb/dibusb-mb.c:31		
			dvb_usb_adapter_frontend_i nit+0xed/0x9a0 drivers/media/usb/dvb- usb/dvb-usb-dvb.c:290 dvb_usb_adapter_init drivers/media/usb/dvb- usb/dvb-usb-init.c:90 [inline] dvb_usb_init drivers/media/usb/dvb- usb/dvb-usb-init.c:186 [inline]		
			dvb_usb_device_init+0x25a 8/0x3760 drivers/media/usb/dvb- usb/dvb-usb-init.c:310 dibusb_probe+0x46/0x250 drivers/media/usb/dvb- usb/dibusb-mb.c:110 		
			Local variable rb created at: dib3000_read_reg+0x86/0x		
			4e0 drivers/media/dvb-frontends/dib3000mb.c:54		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dib3000mb_attach+0x123/ 0x3c0 drivers/media/dvb- frontends/dib3000mb.c:75 8		
			CVE ID: CVE-2024-56769		
Affected Ver	rsion(s): From (in	cluding) 2	6.29 Up to (excluding) 6.1.12	23	
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: tracing: Prevent bad count for tracing_cpumask_write If a large count is provided, it will trigger a warning in bitmap_parse_user. Also check zero for it. CVE ID: CVE-2024-56763	https://git.kern el.org/stable/c/ 03041e474a6a8 f1bfd4b96b164 bb3165c48fa1a 3, https://git.kern el.org/stable/c/ 1cca920af19df5 dd91254e5ff35e 68e911683706, https://git.kern el.org/stable/c/ 3d15f4c244955 8ffe83b4dba306 14ef1cd6937c3	O-LIN-LINU- 200125/945
Affected Ver	rsion(s): From (in	cluding) 3	3 Up to (excluding) 5.4.288		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sched: netem: account for backlog updates from child qdisc In general, 'qlen' of any classful qdisc should keep track of the number of packets that the qdisc itself and all of its children holds. In case of netem, 'qlen' only accounts for the packets in its internal tfifo. When netem is used with a child qdisc, the child qdisc can use 'qdisc_tree_reduce_backlog' to inform its parent, netem, about created or dropped SKBs. This	https://git.kern el.org/stable/c/ 10df49cfca73df bbdb6c4150d85 9f7e8926ae427, https://git.kern el.org/stable/c/ 216509dda290f 6db92c816dd54 b83c1df9da9e7 6, https://git.kern el.org/stable/c/ 356078a5c55ec 8d2061fcc009fb 8599f5b0527f9	O-LIN-LINU- 200125/946

0-1

4-5

5-6

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
W Carriess	1 donish Date		function updates 'qlen' and the backlog statistics of netem, but netem does not account for changes made by a child qdisc. 'qlen' then indicates the wrong number of packets in the tfifo. If a child qdisc creates new SKBs during enqueue and informs its parent about this, netem's 'qlen' value is increased. When netem dequeues the newly created SKBs from the child, the 'qlen' in netem is not updated. If 'qlen' reaches the configured sch->limit, the enqueue function stops working, even though the tfifo is not full.	T divi	NGIII CID
			Reproduce the bug: Ensure that the sender machine has GSO enabled. Configure netem as root qdisc and tbf as its child on the outgoing interface of the machine as follows: \$ tc qdisc add dev <oif> root handle 1: netem delay 100ms limit 100 \$ tc qdisc add dev <oif> parent 1:0 tbf rate 50Mbit burst 1542 latency 50ms</oif></oif>		
			Send bulk TCP traffic out via this interface, e.g., by running an iPerf3 client on the machine. Check the qdisc statistics: \$ tc -s qdisc show dev <oif> Statistics after 10s of iPerf3</oif>		
			TCP test before the fix (note that netem's backlog > limit, netem stopped accepting packets): qdisc netem 1: root refcnt 2		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			limit 1000 delay 100ms Sent 2767766 bytes 1848 pkt (dropped 652, overlimits 0 requeues 0) backlog 4294528236b 1155p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 2767766 bytes 1848 pkt (dropped 327, overlimits 7601 requeues 0) backlog 0b 0p requeues 0		
			Statistics after the fix: qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 37766372 bytes 24974 pkt (dropped 9, overlimits 0 requeues 0) backlog 0b 0p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 37766372 bytes 24974 pkt (dropped 327, overlimits 96017 requeues 0) backlog 0b 0p requeues 0		
			tbf segments the GSO SKBs (tbf_segment) and updates the netem's 'qlen'. The interface fully stops transferring packets and "locks". In this case, the child qdisc and tfifo are empty, but 'qlen' indicates the tfifo is at its limit and no more packets are accepted.		
			This patch adds a counter for the entries in the tfifo. Netem's 'qlen' is only decreased when a packet is returned by its dequeue function, and not during enqueuing into the child qdisc. External updates to 'qlen' are thus		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accounted for and only the behavior of the backlog statistics changes. As in other qdiscs, 'qlen' then keeps track of how many packets are held in netem and all of its children. As before, sch->limit remains as the maximum number of packets in the tfifo. The same applies to netem's backlog statistics. CVE ID: CVE-2024-56770		
Affected Vers	ion(s): From (inc	cluding) 4.	10 Up to (excluding) 4.14.29	19	
Allocation of Resources Without Limits or Throttling	02-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: s5p_cec: limit msg.len to CEC_MAX_MSG_SIZE I expect that the hardware will have limited this to 16, but just in case it hasn't, check for this corner case. CVE ID: CVE-2022-49035	https://git.kern el.org/stable/c/ 1609231f86760 c1f6a429de791 3dd795b9faa08 c, https://git.kern el.org/stable/c/ 2654e785bd4aa 2439cdffbe7dc1 ea30a0eddbfe4, https://git.kern el.org/stable/c/ 4a449430ecfb1 99b99ba58af63 c467eb53500b3	O-LIN-LINU- 200125/947
Affected Vers	sion(s): From (inc	cluding) 4	15 Up to (excluding) 4.19.26	55	
Allocation of Resources Without Limits or Throttling	02-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: s5p_cec: limit msg.len to CEC_MAX_MSG_SIZE I expect that the hardware will have limited this to 16, but just in case it hasn't, check for this corner case. CVE ID: CVE-2022-49035	https://git.kern el.org/stable/c/ 1609231f86760 c1f6a429de791 3dd795b9faa08 c, https://git.kern el.org/stable/c/ 2654e785bd4aa 2439cdffbe7dc1 ea30a0eddbfe4, https://git.kern el.org/stable/c/ 4a449430ecfb1 99b99ba58af63 c467eb53500b3	O-LIN-LINU- 200125/948

4-5

5-6

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				9	
Affected Ver	sion(s): From (in	cluding) 4	19.295 Up to (excluding) 4.2	20	
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: quota: flush quota_release_work upon quota writeback One of the paths quota writeback is called from is: freeze_super() sync_filesystem() ext4_sync_fs() dquot_writeback_dquots() Since we currently don't always flush the quota_release_work queue in this path, we can end up with the following race: 1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state: ext4_journal_check_start+0x 28/0x110 [ext4] (unreliable) ext4_journal_start_sb+0x6 4/0x1c0 [ext4] ext4_release_dquot+0x90/0 x1d0 [ext4]	https://git.kern el.org/stable/c/ 3e6ff207cd5bd9 24ad94cd1a7c6 33bcdac0ba1cb, https://git.kern el.org/stable/c/ 6f3821acd7c31 4314599924808 7de5fb4b48cf26 , https://git.kern el.org/stable/c/ 8ea87e3479225 8825d290f4dc5 216276e91cb22 4	O-LIN-LINU- 200125/949

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			quota_release_workfn+0x43 c/0x4d0 Which is the following line:		
			WARN_ON(sb- >s_writers.frozen == SB_FREEZE_COMPLETE);		
			Which ultimately results in generic/390 failing due to dmesg noise. This was detected on powerpc machine 15 cores.		
			To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze.		
			CVE ID: CVE-2024-56780		
Affected Vers	sion(s): From (inc	cluding) 4.	19.325 Up to (excluding) 4.2	20	
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a	https://git.kern el.org/stable/c/ 6ea15205d7e2b 811fbbdf79783f 686f58abfb4b7, https://git.kern el.org/stable/c/ d2f090ea57f8d6 587e09d4066f7 40a8617767b3d , https://git.kern el.org/stable/c/ d8e4771f99c04	O-LIN-LINU- 200125/950
ACC . LY		1 1:) 4	double free. CVE ID: CVE-2024-56766	00a1873235704 b28bb803c83d1 7	
Affected Vers	sion(s): From (inc	ciuaing) 4.	2 Up to (excluding) 6.1.123		
NULL Pointer Dereference	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: dmaengine: at_xdmac: avoid null_prt_deref in at_xdmac_prep_dma_memse	https://git.kern el.org/stable/c/ 54376d8d2659 6f98ed7432a78 8314bb9154bf3 e3, https://git.kern	O-LIN-LINU- 200125/951

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The at_xdmac_memset_create_d esc may return NULL, which will lead to a null pointer dereference. For example, the len input is error, or the atchan->free_descs_list is empty and memory is exhausted. Therefore, add check to avoid this. CVE ID: CVE-2024-56767	el.org/stable/c/ c43ec96e8d343 99bd9dab2f2dc 316b904892133 f, https://git.kern el.org/stable/c/ e658f1c133b85 4b2ae79914730 1d82dddb8f316 2	
Affected Vers	ion(s): From (inc	cluding) 4	20 Up to (excluding) 5.4.224		
Allocation of Resources Without Limits or Throttling	02-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: s5p_cec: limit msg.len to CEC_MAX_MSG_SIZE I expect that the hardware will have limited this to 16, but just in case it hasn't, check for this corner case. CVE ID: CVE-2022-49035	https://git.kern el.org/stable/c/ 1609231f86760 c1f6a429de791 3dd795b9faa08 c, https://git.kern el.org/stable/c/ 2654e785bd4aa 2439cdffbe7dc1 ea30a0eddbfe4, https://git.kern el.org/stable/c/ 4a449430ecfb1 99b99ba58af63 c467eb53500b3	O-LIN-LINU- 200125/952
Affected Vers	ion(s): From (inc	cluding) 4	6 Up to (excluding) 5.15.174		
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure.	https://git.kern el.org/stable/c/ 40725c5fabee80 4fecce41d4d5c5 bae80c45e1c4, https://git.kern el.org/stable/c/ 831214f77037d e02afc287eae93 ce97f218d8c04, https://git.kern el.org/stable/c/ 8ab73ac97c0fa5 28f66eeccd9bb5 3eb6eb7d20dc	O-LIN-LINU- 200125/953

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-56776		
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers in sti_gdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. CVE ID: CVE-2024-56777	https://git.kern el.org/stable/c/ 3cf2e7c448e246 f7e700c7aa4745 0d1e27579559, https://git.kern el.org/stable/c/ 997b64c3f4c18 27c5cfda8ae7f5 d13f78d28b541, https://git.kern el.org/stable/c/ b79612ed6bc1a 184c45427105c 851b5b2d4342c a	O-LIN-LINU- 200125/954
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers in sti_hqvdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. CVE ID: CVE-2024-56778	·	O-LIN-LINU- 200125/955
Affected Vers	sion(s): From (inc	cluding) 5.	10.195 Up to (excluding) 5.1	0.231	
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: quota: flush quota_release_work upon quota writeback One of the paths quota writeback is called from is:	https://git.kern el.org/stable/c/ 3e6ff207cd5bd9 24ad94cd1a7c6 33bcdac0ba1cb, https://git.kern el.org/stable/c/ 6f3821acd7c31 4314599924808 7de5fb4b48cf26 , https://git.kern	O-LIN-LINU- 200125/956
,	,		One of the paths quota	6f3821acd7c32 431459992480	i 08 26

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sync_filesystem() ext4_sync_fs()	el.org/stable/c/ 8ea87e3479225 8825d290f4dc5	
			dquot_writeback_dquots()	216276e91cb22	
			Since we currently don't always flush the quota_release_work queue in this path, we can end up with the following race:		
			1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state:		
			ext4_journal_check_start+0x 28/0x110 [ext4] (unreliable)		
			_ext4_journal_start_sb+0x6 4/0x1c0 [ext4]		
			ext4_release_dquot+0x90/0 x1d0 [ext4]		
			quota_release_workfn+0x43 c/0x4d0		
			Which is the following line:		
			WARN_ON(sb- >s_writers.frozen == SB_FREEZE_COMPLETE);		
			Which ultimately results in generic/390 failing due to dmesg noise. This was detected on powerpc machine 15 cores.		

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze.		
			CVE ID: CVE-2024-56780		
Affected Vers	sion(s): From (inc	cluding) 5.	10.231 Up to (excluding) 5.1	1	
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free. CVE ID: CVE-2024-56766	https://git.kern el.org/stable/c/ 6ea15205d7e2b 811fbbdf79783f 686f58abfb4b7, https://git.kern el.org/stable/c/ d2f090ea57f8d6 587e09d4066f7 40a8617767b3d , https://git.kern el.org/stable/c/ d8e4771f99c04 00a1873235704 b28bb803c83d1 7	O-LIN-LINU- 200125/957
Affected Vers	sion(s): From (inc	cluding) 5.	11 Up to (excluding) 5.15.17	74	
Missing Release of Memory after Effective Lifetime	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix nfs4_openowner leak when concurrent nfsd4_open occur The action force umount(umount -f) will attempt to kill all rpc_task even umount operation may ultimately fail if some files remain open. Consequently, if an action attempts to open a file, it can potentially send two rpc_task to nfs server.	https://git.kern el.org/stable/c/ 0ab0a3ad24e97 0e894abcac58f8 5c332d1726749 , https://git.kern el.org/stable/c/ 2d505a801e574 28057563762f6 7a5a62009b260 0, https://git.kern el.org/stable/c/ 37dfc81266d3a 32294524bfadd 3396614f8633e e	O-LIN-LINU- 200125/958

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			thread1 thread2 open("file")		
			nfs4_do_open _nfs4_do_open _nfs4_open_and_get_state _nfs4_proc_open nfs4_run_open_task /* rpc_task1 */ rpc_run_task		
			rpc_wait_for_completion_tas k		
			umount - f		
			nfs_umount_begin		
			rpc_killall_tasks		
			rpc_signal_task rpc_task1 been wakeup and return -512 _nfs4_do_open // while loop		
			 nfs4_run_open_task /* rpc_task2 */ rpc_run_task		
			rpc_wait_for_completion_tas k		
			While processing an open request, nfsd will first attempt to find or allocate an nfs4_openowner. If it finds an nfs4_openowner that is not marked as		
			marked as NFS4_OO_CONFIRMED, this nfs4_openowner will released. Since two rpc_task can attempt to open the same file		
			simultaneously from the client to server, and because two instances of nfsd can run		

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			concurrently, this situation can lead to lots of memory leak. Additionally, when we echo 0 to /proc/fs/nfsd/threads, warning will be triggered.		
			NFS SERVER nfsd1 nfsd2 echo 0 > /proc/fs/nfsd/threads		
			nfsd4_open nfsd4_process_open1		
			find_or_alloc_open_stateow ner // alloc oo1, stateid1 nfsd4_open		
			nfsd4_process_open1		
			find_or_alloc_open_stateow ner // find oo1, without NFS4_OO_CONFIRMED		
			release_openowner		
			unhash_openowner_locked		
			list_del_init(&oo- >oo_perclient)		
			alloc_stateowner // alloc oo2		
			nfsd4_process_open2 init_open_stateid // associate oo1 // with stateid1, stateid1 LEAK!!! nfs4_get_vfs_file // alloc nfsd_file1 and nfsd_file_mark1 // all LEAK!!!		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nfsd4_process_open2 		
			write_threads 		
			nfsd_destroy_serv		
			nfsd_shutdown_net		
			nfs4_state_shutdown_net		
			nfs4_state_destroy_net		
			destroy_client		
			destroy_client		
			won't find oo1!!!		
			nfsd_shutdown_generic		
			nfsd_file_cache_shutdown		
			kmem_cache_destroy for nfsd_file_slab and nfsd_file_mark_slab // bark since nfsd_file1 // and nfsd_file_mark1 // still alive		
			======================================		
1			Slab 0xffd4000004438a80 objects=34 used=1		

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fp=0xff11000110e2ad28 flags=0x17ffffc0000240(wo rkingset head node=0 zone =2 lastcpupid=0x1fffff) CPU: 4 UID: 0 PID: 757 Comm: sh Not tainted 6.12.0-rc6+ #19 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.1-2.fc37 04/01/2014 Call Trace: <task> dumtruncated CVE ID: CVE-2024-56779</task>		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: powerpc/prom_init: Fixup missing powermac #sizecells On some powermacs `escc` nodes are missing `#sizecells` properties, which is deprecated and now triggers a warning at boot since commit 045b14ca5c36 ("of: WARN on deprecated #addresscells/#size-cells handling"). For example: Missing '#size-cells' in /pci@f2000000/macio@c/escc@13000 WARNING: CPU: 0 PID: 0 at drivers/of/base.c:133 of_bus_n_size_cells+0x98/0 x108 Hardware name: PowerMac3,1 7400 0xc0209 PowerMac Call Trace:	https://git.kern el.org/stable/c/ 0b94d838018fb 0a824e0cd3149 034928c99fb1b 7, https://git.kern el.org/stable/c/ 296a109fa7711 0ba5267fe0e90 a26005eecc272 6, https://git.kern el.org/stable/c/ 691284c2cd33ff aa0b35ce53b32 86b90621e9dc9	O-LIN-LINU- 200125/959

CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of_bus_n_size_cells+0x98/0 x108 (unreliable)		
			of_bus_default_count_cells+ 0x40/0x60		
			of_get_address+0xc8/0x2 1c		
			of_address_to_resource+0 x5c/0x228		
			pmz_init_port+0x5c/0x2ec		
			pmz_probe.isra.0+0x144/0x 1e4		
			pmz_console_init+0x10/0x4 8 console_init+0xcc/0x138		
			start_kernel+0x5c4/0x694		
			As powermacs boot via prom_init it's possible to add the missing properties to the device tree during boot, avoiding the warning. Note that `escc-legacy` nodes are also missing `#size-cells` properties, but they are skipped by the macio driver, so leave them alone.		
			Depends-on: 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling")		
			CVE ID: CVE-2024-56781		
			In the Linux kernel, the following vulnerability has been resolved:	https://git.kern el.org/stable/c/ 01575f2ff8ba57 8a3436f230668	O I IN I INII
N/A	08-Jan-2025	5.5	MIPS: Loongson64: DTS: Really fix PCIe port nodes for ls7a	bd056dc2eb823 , https://git.kern el.org/stable/c/	O-LIN-LINU- 200125/960
			Fix the dtc warnings:	4fbd66d8254ce	

CVSSv3 Scoring Scale
* stands for all versions 3-4 8-9 9-10 0-1 2-3 4-5 5-6 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arch/mips/boot/dts/loongs on/ls7a-pch.dtsi:68.16- 416.5: Warning (interrupt_provider): /bus@10000000/pci@1a0 00000: '#interrupt-cells' found, but node is not an interrupt provider	dfd1218393f39 d83b6c07a0191 7, https://git.kern el.org/stable/c/ 5a2eaa3ad2b80 3c7ea442c6db7 379466ee73c02	
			arch/mips/boot/dts/loongs on/ls7a-pch.dtsi:68.16- 416.5: Warning (interrupt_provider): /bus@10000000/pci@1a0 00000: '#interrupt-cells' found, but node is not an interrupt provider		
			arch/mips/boot/dts/loongs on/loongson64g_4core_ls7a .dtb: Warning (interrupt_map): Failed prerequisite 'interrupt_provider'		
			And a runtime warning introduced in commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"):		
			WARNING: CPU: 0 PID: 1 at drivers/of/base.c:106 of_bus_n_addr_cells+0x9c/0 xe0 Missing '#address-cells' in /bus@10000000/pci@1a0 00000/pci_bridge@9,0		
			The fix is similar to commit d89a415ff8d5 ("MIPS: Loongson64: DTS: Fix PCIe port nodes for ls7a"), which has fixed the issue for ls2k (despite its subject mentions ls7a).		
			CVE ID: CVE-2024-56785		

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: add a sanity check for btrfs root in btrfs_search_slot() Syzbot reports a null-ptr-deref in btrfs_search_slot(). The reproducer is using rescue=ibadroots, and the extent tree root is corrupted thus the extent tree is NULL. When scrub tries to search the extent tree to gather the needed extent info, btrfs_search_slot() doesn't check if the target root is NULL or not, resulting the null-ptr-deref. Add sanity check for btrfs root before using it in btrfs_search_slot(). CVE ID: CVE-2024-56774	https://git.kern el.org/stable/c/ 3ed51857a50f5 30ac7a1482e06 9dfbd1298558d 4, https://git.kern el.org/stable/c/ 757171d1369b3 b47f36932d40a 05a0715496dca b, https://git.kern el.org/stable/c/ 93992c3d9629b 02dccf6849238 559d5c24f2dece	0-LIN-LINU- 200125/961
Affected Vers	sion(s): From (in	cluding) 5.	11 Up to (excluding) 5.15.17	⁷ 5	
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sched: netem: account for backlog updates from child qdisc In general, 'qlen' of any classful qdisc should keep track of the number of packets that the qdisc itself and all of its children holds. In case of netem, 'qlen' only accounts for the packets in its internal tfifo. When netem is used with a child qdisc, the child	https://git.kern el.org/stable/c/ 10df49cfca73df bbdb6c4150d85 9f7e8926ae427, https://git.kern el.org/stable/c/ 216509dda290f 6db92c816dd54 b83c1df9da9e7 6, https://git.kern el.org/stable/c/ 356078a5c55ec 8d2061fcc009fb 8599f5b0527f9	O-LIN-LINU- 200125/962

0-1

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			qdisc can use 'qdisc_tree_reduce_backlog' to inform its parent, netem, about created or dropped SKBs. This function updates 'qlen' and the backlog statistics of netem, but netem does not account for changes made by a child qdisc. 'qlen' then indicates the wrong number of packets in the tfifo. If a child qdisc creates new SKBs during enqueue and informs its parent about this, netem's 'qlen' value is increased. When netem dequeues the newly created SKBs from the child, the 'qlen' in netem is not updated. If 'qlen' reaches the configured sch->limit, the enqueue function stops working, even though the tfifo is not full.		
			Reproduce the bug: Ensure that the sender machine has GSO enabled. Configure netem as root qdisc and tbf as its child on the outgoing interface of the machine as follows: \$ tc qdisc add dev <oif> root handle 1: netem delay 100ms limit 100 \$ tc qdisc add dev <oif> parent 1:0 tbf rate 50Mbit burst 1542 latency 50ms Send bulk TCP traffic out via</oif></oif>		
			this interface, e.g., by running an iPerf3 client on the machine. Check the qdisc statistics: \$ tc -s qdisc show dev <oif> Statistics after 10s of iPerf3 TCP test before the fix (note</oif>		

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	that netem's backlog > limit, netem stopped accepting packets): qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 2767766 bytes 1848 pkt (dropped 652, overlimits 0 requeues 0) backlog 4294528236b 1155p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 2767766 bytes 1848 pkt (dropped 327, overlimits 7601 requeues 0) backlog 0b 0p requeues 0 Statistics after the fix: qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 37766372 bytes 24974 pkt (dropped 9, overlimits 0 requeues 0) backlog 0b 0p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat	Patch	NCIIPC ID
			50ms Sent 37766372 bytes 24974 pkt (dropped 327, overlimits 96017 requeues 0) backlog 0b 0p requeues 0		
			tbf segments the GSO SKBs (tbf_segment) and updates the netem's 'qlen'. The interface fully stops transferring packets and "locks". In this case, the child qdisc and tfifo are empty, but 'qlen' indicates the tfifo is at its limit and no more packets are accepted.		
			This patch adds a counter for the entries in the tfifo. Netem's 'qlen' is only decreased when a		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packet is returned by its dequeue function, and not during enqueuing into the child qdisc. External updates to 'qlen' are thus accounted for and only the behavior of the backlog statistics changes. As in other qdiscs, 'qlen' then keeps track of how many packets are held in netem and all of its children. As before, sch->limit remains as the maximum number of packets in the tfifo. The same applies to netem's backlog statistics. CVE ID: CVE-2024-56770		
Affected Vers	sion(s): From (inc	cluding) 5.	11 Up to (excluding) 5.15.78	3	
Allocation of Resources Without Limits or Throttling	02-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: s5p_cec: limit msg.len to CEC_MAX_MSG_SIZE I expect that the hardware will have limited this to 16, but just in case it hasn't, check for this corner case. CVE ID: CVE-2022-49035	https://git.kern el.org/stable/c/ 1609231f86760 c1f6a429de791 3dd795b9faa08 c, https://git.kern el.org/stable/c/ 2654e785bd4aa 2439cdffbe7dc1 ea30a0eddbfe4, https://git.kern el.org/stable/c/ 4a449430ecfb1 99b99ba58af63 c467eb53500b3 9	O-LIN-LINU- 200125/963
Affected Vers	sion(s): From (inc	cluding) 5.	15.132 Up to (excluding) 5.1	5.174	l
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: quota: flush quota_release_work upon quota writeback One of the paths quota writeback is called from is:	https://git.kern el.org/stable/c/ 3e6ff207cd5bd9 24ad94cd1a7c6 33bcdac0ba1cb, https://git.kern el.org/stable/c/ 6f3821acd7c31 4314599924808 7de5fb4b48cf26	O-LIN-LINU- 200125/964

CVSSv3 Scoring Scale	
* stands for all versions	

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			freeze_super() sync_filesystem() ext4_sync_fs() dquot_writeback_dquots() Since we currently don't always flush the quota_release_work queue in this path, we can end up with the following race:	https://git.kern el.org/stable/c/ 8ea87e3479225 8825d290f4dc5 216276e91cb22 4	
			1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state:		
			ext4_journal_check_start+0x 28/0x110 [ext4] (unreliable) ext4_journal_start_sb+0x6 4/0x1c0 [ext4] ext4_release_dquot+0x90/0		
			x1d0 [ext4] quota_release_workfn+0x43 c/0x4d0 Which is the following line: WARN_ON(sb- >s_writers.frozen == SB_FREEZE_COMPLETE);		
			Which ultimately results in generic/390 failing due to dmesg noise. This was detected on		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			powerpc machine 15 cores.		
			To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze.		
			CVE ID: CVE-2024-56780		
Affected Vers	sion(s): From (inc	cluding) 5.	15.174 Up to (excluding) 5.1	.6	l
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free. CVE ID: CVE-2024-56766	https://git.kern el.org/stable/c/ 6ea15205d7e2b 811fbbdf79783f 686f58abfb4b7, https://git.kern el.org/stable/c/ d2f090ea57f8d6 587e09d4066f7 40a8617767b3d , https://git.kern el.org/stable/c/ d8e4771f99c04 00a1873235704 b28bb803c83d1 7	O-LIN-LINU- 200125/965
Affected Vers	sion(s): From (inc	cluding) 5.	16 Up to (excluding) 6.0.8		
Allocation of Resources Without Limits or Throttling	02-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: s5p_cec: limit msg.len to CEC_MAX_MSG_SIZE I expect that the hardware will have limited this to 16, but just in case it hasn't, check for this corner case. CVE ID: CVE-2022-49035	https://git.kern el.org/stable/c/ 1609231f86760 c1f6a429de791 3dd795b9faa08 c, https://git.kern el.org/stable/c/ 2654e785bd4aa 2439cdffbe7dc1 ea30a0eddbfe4, https://git.kern el.org/stable/c/ 4a449430ecfb1 99b99ba58af63 c467eb53500b3 9	O-LIN-LINU- 200125/966
Affected Vers	sion(s): From (inc	cluding) 5.	16 Up to (excluding) 6.1.120		
NULL Pointer	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has	https://git.kern el.org/stable/c/	0-LIN-LINU- 200125/967

4-5

5-6

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			been resolved: btrfs: add a sanity check for btrfs root in btrfs_search_slot() Syzbot reports a null-ptr-deref in btrfs_search_slot(). The reproducer is using rescue=ibadroots, and the extent tree root is corrupted thus the extent tree is NULL. When scrub tries to search the extent tree to gather the needed extent info, btrfs_search_slot() doesn't check if the target root is NULL or not, resulting the null-ptr-deref. Add sanity check for btrfs root before using it in btrfs_search_slot(). CVE ID: CVE-2024-56774	3ed51857a50f5 30ac7a1482e06 9dfbd1298558d 4, https://git.kern el.org/stable/c/ 757171d1369b3 b47f36932d40a 05a0715496dca b, https://git.kern el.org/stable/c/ 93992c3d9629b 02dccf6849238 559d5c24f2dece	
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. CVE ID: CVE-2024-56776	https://git.kern el.org/stable/c/ 40725c5fabee80 4fecce41d4d5c5 bae80c45e1c4, https://git.kern el.org/stable/c/ 831214f77037d e02afc287eae93 ce97f218d8c04, https://git.kern el.org/stable/c/ 8ab73ac97c0fa5 28f66eeccd9bb5 3eb6eb7d20dc	O-LIN-LINU- 200125/968
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential	https://git.kern el.org/stable/c/ 3cf2e7c448e246 f7e700c7aa4745 0d1e27579559,	O-LIN-LINU- 200125/969

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dereference of error pointers in sti_gdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. CVE ID: CVE-2024-56777	https://git.kern el.org/stable/c/ 997b64c3f4c18 27c5cfda8ae7f5 d13f78d28b541, https://git.kern el.org/stable/c/ b79612ed6bc1a 184c45427105c 851b5b2d4342c a	
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers in sti_hqvdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. CVE ID: CVE-2024-56778	https://git.kern el.org/stable/c/ 31c857e7496d3 4e5a32a6f75bc0 24d0b06fd646a, https://git.kern el.org/stable/c/ 6b0d0d6e9d3c2 6697230bf7dc9 e6b52bdb24086 f, https://git.kern el.org/stable/c/ 82a5312f874fb1 8f045d9658e9b d290e3b0621c0	O-LIN-LINU- 200125/970
Missing Release of Memory after Effective Lifetime	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix nfs4_openowner leak when concurrent nfsd4_open occur The action force umount(umount -f) will attempt to kill all rpc_task even umount operation may ultimately fail if some files remain open. Consequently, if an action attempts to open a file, it can potentially send two rpc_task to nfs server.	https://git.kern el.org/stable/c/ 0ab0a3ad24e97 0e894abcac58f8 5c332d1726749 , https://git.kern el.org/stable/c/ 2d505a801e574 28057563762f6 7a5a62009b260 0, https://git.kern el.org/stable/c/ 37dfc81266d3a 32294524bfadd 3396614f8633e e	O-LIN-LINU- 200125/971

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NFS CLIENT thread1 thread2 open("file")		
			nfs4_do_open _nfs4_do_open _nfs4_do_open _nfs4_open_and_get_state _nfs4_proc_open nfs4_run_open_task /* rpc_task1 */ rpc_run_task		
			rpc_wait_for_completion_tas k		
			umount -		
			nfs_umount_begin		
			rpc_killall_tasks		
			rpc_signal_task rpc_task1 been wakeup and return -512 _nfs4_do_open // while loop		
			 nfs4_run_open_task /* rpc_task2 */ rpc_run_task		
			rpc_wait_for_completion_tas k		
			While processing an open request, nfsd will first attempt to find or allocate an nfs4_openowner. If it finds an nfs4_openowner that is not marked as NFS4_OO_CONFIRMED, this nfs4_openowner will		
			released. Since two rpc_task can attempt to open the same file simultaneously from the client to server, and because		

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			two instances of nfsd can run concurrently, this situation can lead to lots of memory leak. Additionally, when we echo 0 to /proc/fs/nfsd/threads, warning will be triggered.		
			NFS SERVER nfsd1 nfsd2 echo 0 > /proc/fs/nfsd/threads		
			nfsd4_open nfsd4_process_open1		
			find_or_alloc_open_stateow ner // alloc oo1, stateid1 nfsd4_open		
			nfsd4_process_open1		
			find_or_alloc_open_stateow ner // find oo1, without NFS4_OO_CONFIRMED		
			release_openowner		
			unhash_openowner_locked		
			list_del_init(&oo- >oo_perclient)		
			alloc_stateowner // alloc oo2		
			nfsd4_process_open2 init_open_stateid // associate oo1 // with stateid1, stateid1 LEAK!!! nfs4_get_vfs_file // alloc nfsd_file1 and		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nfsd_file_mark1 // all LEAK!!!		
			nfsd4_process_open2 		
			write_threads 		
			nfsd_destroy_serv		
			nfsd_shutdown_net		
			nfs4_state_shutdown_net		
			nfs4_state_destroy_net		
			destroy_client		
			destroy_client		
			won't find oo1!!!		
			nfsd_shutdown_generic		
			nfsd_file_cache_shutdown		
			kmem_cache_destroy		
			for nfsd_file_slab		
			and nfsd_file_mark_slab		
			// bark since nfsd_file1		
			// and nfsd_file_mark1		
			// still alive		
			=======================================		
			=======================================		
			BUG nfsd_file (Not tainted): Objects remaining in		
			nfsd_file on kmem_cache_shutdown()		

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Slab 0xffd4000004438a80 objects=34 used=1 fp=0xff11000110e2ad28 flags=0x17ffffc0000240(wo rkingset head node=0 zone =2 lastcpupid=0x1fffff) CPU: 4 UID: 0 PID: 757 Comm: sh Not tainted 6.12.0-rc6+ #19 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.1-2.fc37 04/01/2014 Call Trace: <task> dumtruncated</task>		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: powerpc/prom_init: Fixup missing powermac #sizecells On some powermacs 'escc' nodes are missing '#sizecells' properties, which is deprecated and now triggers a warning at boot since commit 045b14ca5c36 ("of: WARN on deprecated #addresscells/#size-cells handling"). For example: Missing '#size-cells' in /pci@f2000000/macio@c/escc@13000 WARNING: CPU: 0 PID: 0 at drivers/of/base.c:133 of_bus_n_size_cells+0x98/0 x108 Hardware name: PowerMac3,1 7400 0xc0209 PowerMac	https://git.kern el.org/stable/c/ 0b94d838018fb 0a824e0cd3149 034928c99fb1b 7, https://git.kern el.org/stable/c/ 296a109fa7711 0ba5267fe0e90 a26005eecc272 6, https://git.kern el.org/stable/c/ 691284c2cd33ff aa0b35ce53b32 86b90621e9dc9	O-LIN-LINU- 200125/972

CVSSv3 Scoring Scale
* stands for all versions 3-4 8-9 0-1 2-3 4-5 5-6 6-7 7-8 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Call Trace:		
			of_bus_n_size_cells+0x98/0 x108 (unreliable)		
			of_bus_default_count_cells+ 0x40/0x60		
			_of_get_address+0xc8/0x2 1c		
			of_address_to_resource+0 x5c/0x228		
			pmz_init_port+0x5c/0x2ec		
			pmz_probe.isra.0+0x144/0x 1e4		
			pmz_console_init+0x10/0x4 8 console_init+0xcc/0x138		
			start_kernel+0x5c4/0x694		
			As powermacs boot via prom_init it's possible to add the missing properties to the device tree during boot, avoiding the warning. Note that `escc-legacy` nodes are also missing `#size-cells` properties, but they are skipped by the macio driver, so leave them alone.		
			Depends-on: 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling")		
			CVE ID: CVE-2024-56781		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: MIPS: Loongson64: DTS:	https://git.kern el.org/stable/c/ 01575f2ff8ba57 8a3436f230668 bd056dc2eb823	O-LIN-LINU- 200125/973
			Really fix PCIe port nodes for ls7a	, https://git.kern	

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fix the dtc warnings:	el.org/stable/c/ 4fbd66d8254ce dfd1218393f39 d83b6c07a0191	
			arch/mips/boot/dts/loongs on/ls7a-pch.dtsi:68.16- 416.5: Warning (interrupt_provider): /bus@10000000/pci@1a0 00000: '#interrupt-cells' found, but node is not an interrupt provider	7, https://git.kern el.org/stable/c/ 5a2eaa3ad2b80 3c7ea442c6db7 379466ee73c02	
			arch/mips/boot/dts/loongs on/ls7a-pch.dtsi:68.16- 416.5: Warning (interrupt_provider): /bus@10000000/pci@1a0 00000: '#interrupt-cells' found, but node is not an interrupt provider		
			arch/mips/boot/dts/loongs on/loongson64g_4core_ls7a .dtb: Warning (interrupt_map): Failed prerequisite 'interrupt_provider'		
			And a runtime warning introduced in commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"):		
			WARNING: CPU: 0 PID: 1 at drivers/of/base.c:106 of_bus_n_addr_cells+0x9c/0 xe0 Missing '#address-cells' in /bus@10000000/pci@1a0 00000/pci_bridge@9,0		
			The fix is similar to commit d89a415ff8d5 ("MIPS: Loongson64: DTS: Fix PCIe port nodes for ls7a"), which has fixed the issue for ls2k (despite its subject mentions ls7a).		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-56785		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: soc: imx8m: Probe the SoC driver as platform driver With driver_async_probe=* on kernel command line, the following trace is produced because on i.MX8M Plus hardware because the soc-imx8m.c driver calls of_clk_get_by_name() which returns - EPROBE_DEFER because the clock driver is not yet probed. This was not detected during regular testing without driver_async_probe. Convert the SoC code to platform driver and instantiate a platform device in its current device_initcall() to probe the platform driver. Rework .soc_revision callback to always return valid error code and return SoC revision via parameter. This way, if anything in the .soc_revision callback return -EPROBE_DEFER, it gets propagated to .probe and the .probe will get retried later. "	https://git.kern el.org/stable/c/ 2129f6faa5dfe8 c6b87aad11720 bf75edd77d3e4, https://git.kern el.org/stable/c/ 997a3c04d7fa3 d1d385c146913 50d096fada648 c, https://git.kern el.org/stable/c/ 9cc832d37799d bea950c4c8a34 721b02b8b5a8ff	O-LIN-LINU- 200125/974

^{*} stands for all versions

/0x180 CPU: 1 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.11.0-next-20240924- 00002-g2062bb554dea #603 Hardware name: DH electronics i.MXBM Plus DHCOM Premium Developer Kit (3) (DT) pstate: 20000005 (nzCv daif -PAN-UAO -TCO -DIT -SSBS BTYPE) pc :: imx8mm_soc_revision+0xd /0x180 lr :: imx8mm_soc_revision+0xd 0/0x180 sp : fff8000821fbcc0 x29: fff8000821fbce0 x28: 000000000000000000 x27: fff800081810120 x26: fff80008183970 x25: 000000000000000000 x24: 000000000000000000 x24: 000000000000000000 x24: fff800081411 x23: fff80008143970 x25: fff8000818740248 x22: fff8000818780000 x19: 000000000000000001 x18: ffffffffffffffffffffffffffffffffffff
: Illillillillidib x0 : ffffffffffffffdfb Call trace:

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			imx8mm_soc_revision+0xdc /0x180 imx8_soc_init+0xb0/0x1e0 do_one_initcall+0x94/0x1a 8 kernel_init_freeable+0x240 /0x2a8 kernel_init+0x28/0x140 ret_from_fork+0x10/0x20[end trace 00000000000000000] SoC: i.MX8MP revision 1.1 " CVE ID: CVE-2024-56787		
Affected Ver	sion(s): From (inc	cluding) 5.	16 Up to (excluding) 6.1.121		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sched: netem: account for backlog updates from child qdisc In general, 'qlen' of any classful qdisc should keep track of the number of packets that the qdisc itself and all of its children holds. In case of netem, 'qlen' only accounts for the packets in its internal tfifo. When netem is used with a child qdisc, the child qdisc can use 'qdisc_tree_reduce_backlog' to inform its parent, netem, about created or dropped SKBs. This function updates 'qlen' and the backlog statistics of netem, but netem does not account for changes made by a child qdisc. 'qlen' then indicates the wrong number of packets in the tfifo. If a child qdisc creates new	https://git.kern el.org/stable/c/ 10df49cfca73df bbdb6c4150d85 9f7e8926ae427, https://git.kern el.org/stable/c/ 216509dda290f 6db92c816dd54 b83c1df9da9e7 6, https://git.kern el.org/stable/c/ 356078a5c55ec 8d2061fcc009fb 8599f5b0527f9	O-LIN-LINU- 200125/975

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SKBs during enqueue and informs its parent about this, netem's 'qlen' value is increased. When netem dequeues the newly created SKBs from the child, the 'qlen' in netem is not updated. If 'qlen' reaches the configured sch->limit, the enqueue function stops working, even though the tfifo is not full.		
			Reproduce the bug: Ensure that the sender machine has GSO enabled. Configure netem as root qdisc and tbf as its child on the outgoing interface of the machine as follows: \$ tc qdisc add dev <oif> root handle 1: netem delay 100ms limit 100 \$ tc qdisc add dev <oif> parent 1:0 tbf rate 50Mbit burst 1542 latency 50ms</oif></oif>		
			Send bulk TCP traffic out via this interface, e.g., by running an iPerf3 client on the machine. Check the qdisc statistics: \$ tc -s qdisc show dev <oif></oif>		
			Statistics after 10s of iPerf3 TCP test before the fix (note that netem's backlog > limit, netem stopped accepting packets): qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 2767766 bytes 1848 pkt (dropped 652, overlimits 0 requeues 0) backlog 4294528236b 1155p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sent 2767766 bytes 1848 pkt (dropped 327, overlimits 7601 requeues 0) backlog 0b 0p requeues 0		
			Statistics after the fix: qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 37766372 bytes 24974 pkt (dropped 9, overlimits 0 requeues 0) backlog 0b 0p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 37766372 bytes 24974 pkt (dropped 327, overlimits 96017 requeues 0) backlog 0b 0p requeues 0		
			tbf segments the GSO SKBs (tbf_segment) and updates the netem's 'qlen'. The interface fully stops transferring packets and "locks". In this case, the child qdisc and tfifo are empty, but 'qlen' indicates the tfifo is at its limit and no more packets are accepted.		
			This patch adds a counter for the entries in the tfifo. Netem's 'qlen' is only decreased when a packet is returned by its dequeue function, and not during enqueuing into the child qdisc. External updates to 'qlen' are thus accounted for and only the behavior of the backlog statistics changes. As in other qdiscs, 'qlen' then keeps track of how many packets are held in		
			netem and all of its children. As before, sch->limit remains as the		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): From (inc	cluding) 5	maximum number of packets in the tfifo. The same applies to netem's backlog statistics. CVE ID: CVE-2024-56770 18 Up to (excluding) 6.1.123		
Use After Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries/vas: Add close() callback in vas_vm_ops struct The mapping VMA address is saved in VAS window struct when the paste address is mapped. This VMA address is used during migration to unmap the paste address if the window is active. The paste address mapping will be removed when the window is closed or with the munmap(). But the VMA address in the VAS window is not updated with munmap() which is causing invalid access during migration. The KASAN report shows: [16386.254991] BUG: KASAN: slab-use-after-free in reconfig_close_windows+0x 1a0/0x4e8 [16386.255043] Read of size 8 at addr c00000014a819670 by task drmgr/696928 [16386.255096] CPU: 29 UID: 0 PID: 696928 Comm: drmgr Kdump: loaded Tainted: G B 6.11.0-rc5-nxgzip #2 [16386.255128] Tainted:	https://git.kern el.org/stable/c/ 05aa156e156ef 3168e7ab8a687 21945196495c1 7, https://git.kern el.org/stable/c/ 6d9cd27105459 f169993a4c5f21 6499a946dbf34, https://git.kern el.org/stable/c/ 8b2282b508452 1254a2cd9742a 3f4e1d5b77f843	O-LIN-LINU- 200125/976

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakiless	audish Date	CV33V3	[B]=BAD_PAGE [16386.255148] Hardware name: IBM,9080-HEX Power11 (architected) 0x820200 0xf000007 of:IBM,FW1110.00 (NH1110_016) hv:phyp pSeries [16386.255181] Call Trace: [16386.255202] [c00000016b297660] [c000000018ad0ac] dump_stack_lvl+0x84/0xe8 (unreliable) [16386.255246] [c00000016b297690] [c000000006e8a90] print_report+0x19c/0x764 [16386.255285] [c00000016b297760] [c000000006e9490] kasan_report+0x128/0x1f8 [16386.255309] [c00000016b297880] [c00000016b297880] [c00000016b297880] [c00000016b2978a0] [c000000016b2978a0] [c000000016b2978a0] [c000000016b2978a0] [c00000016b2978a0] [c000000016b2978a0] [c000000016b2978a0] [c000000016b2978a0] [c000000016b2978a0] [c00000000013f898] reconfig_close_windows+0x 1a0/0x4e8 [16386.255343] [c00000016b297990] [c0000000000128848] pseries_migration_handler+0x3 a4/0x3fc [16386.255368] [c00000016b297a90] [c000000000128848] pseries_migrate_partition+0 x4c/0x4c4 [16386.256136] Allocated by task 696554 on cpu 31 at 16377.277618s: [16386.256149] kasan_save_stack+0x34/0x 68	rawii	
			[16386.256163] kasan_save_track+0x34/0x		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[16386.256175] kasan_save_alloc_info+0x58 /0x74 [16386.256196]kasan_slab_alloc+0xb8/0x dc [16386.256209] kmem_cache_alloc_noprof+ 0x200/0x3d0 [16386.256225] vm_area_alloc+0x44/0x150 [16386.256245] mmap_region+0x214/0x10 c4 [16386.256265] do_mmap+0x5fc/0x750 [16386.256277] vm_mmap_pgoff+0x14c/0x 24c [16386.256292] ksys_mmap_pgoff+0x20c/0 x348 [16386.256303] sys_mmap+0xd0/0x160		
			[16386.256350] Freed by task 0 on cpu 31 at 16386.204848s: [16386.256363] kasan_save_stack+0x34/0x 68 [16386.256374] kasan_save_track+0x34/0x 80 [16386.256384] kasan_save_free_info+0x64/0x10c [16386.256396]kasan_slab_free+0x120/0 x204 [16386.256415] kmem_cache_free+0x128/0 x450 [16386.256428] vm_area_free_rcu_cb+0xa8/0xd8 [16386.256441] rcu_do_batch+0x2c8/0xcf0 [16386.256458] rcu_core+0x378/0x3c4 [16386.256473]		

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handle_softirqs+0x20c/0x6 0c [16386.256495] do_softirq_own_stack+0x6c /0x88 [16386.256509] do_softirq_own_stack+0x58 /0x88 [16386.256521] irq_exit_rcu+0x1a4/0x20c [16386.256533] irq_exit+0x20/0x38 [16386.256544] interrupt_async_exit_prepar e.constprop.0+0x18/0x2c 		
			[16386.256717] Last potentially related work creation: [16386.256729] kasan_save_stack+0x34/0x 68 [16386.256741]kasan_record_aux_stack+0 xcc/0x12c [16386.256753]call_rcu_common.constpro p.0+0x94/0xd04 [16386.256766] vm_area_free+0x28/0x3c [16386.256778] remove_vma+0xf4/0x114 [16386.256797] do_vmi_align_munmap.cons tprop.0+0x684/0x870 [16386.256811]vm_munmap+0xe0/0x1f8 [16386.256821] sys_munmap+0x54/0x6c [16386.256830] system_call_exception+0x1a 0/0x4a0 [16386.256841] system_call_vectored_comm on+0x15c/0x2ec		
			[16386.256868] The buggy address belongs to the object at c00000014a819670 which belongs to		

0-1

4-5

5-6

6-7

9-10

8-9

7-8

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the cache vm_area_struct of size 168 [16386.256887] The buggy address is located 0 bytes inside of freed 168-byte region [c00000014a819670, c000000014a819718]		
			[16386.256915] The buggy address belongs to the physical page: [16386.256928] page: refcount:1 mapcount:0 mapping:000000000000000000000000000000000000		
Affacted Vor	sion(s). From (in	cluding) 5	CVE ID: CVE-2024-56765	207	
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: quota: flush quota_release_work upon quota writeback One of the paths quota writeback is called from is: freeze_super() sync_filesystem() ext4_sync_fs() dquot_writeback_dquots() Since we currently don't always flush the quota_release_work queue in this path, we can end up	https://git.kern el.org/stable/c/ 3e6ff207cd5bd9 24ad94cd1a7c6 33bcdac0ba1cb, https://git.kern el.org/stable/c/ 6f3821acd7c31 4314599924808 7de5fb4b48cf26 , https://git.kern el.org/stable/c/ 8ea87e3479225 8825d290f4dc5 216276e91cb22 4	O-LIN-LINU- 200125/977

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the following race:		
			1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue.		
			3. Freeze completes. 4. Kernel eventually tries to flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state:		
			ext4_journal_check_start+0x 28/0x110 [ext4] (unreliable)		
			_ext4_journal_start_sb+0x6 4/0x1c0 [ext4]		
			ext4_release_dquot+0x90/0 x1d0 [ext4]		
			quota_release_workfn+0x43 c/0x4d0		
			Which is the following line:		
			WARN_ON(sb- >s_writers.frozen == SB_FREEZE_COMPLETE);		
			Which ultimately results in generic/390 failing due to dmesg noise. This was detected on powerpc machine 15 cores.		
			To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze.		
			CVE ID: CVE-2024-56780		

CVSSv3 Scoring Scale	0-1
* stands for all versions	

5-6

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	ion(s): From (inc	cluding) 5.	4.287 Up to (excluding) 5.5	L	L
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free. CVE ID: CVE-2024-56766	https://git.kern el.org/stable/c/ 6ea15205d7e2b 811fbbdf79783f 686f58abfb4b7, https://git.kern el.org/stable/c/ d2f090ea57f8d6 587e09d4066f7 40a8617767b3d , https://git.kern el.org/stable/c/ d8e4771f99c04 00a1873235704 b28bb803c83d1 7	O-LIN-LINU- 200125/978
Affected Vers	ion(s): From (inc	cluding) 5.	5 Up to (excluding) 5.10.154		
Allocation of Resources Without Limits or Throttling	02-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: s5p_cec: limit msg.len to CEC_MAX_MSG_SIZE I expect that the hardware will have limited this to 16, but just in case it hasn't, check for this corner case. CVE ID: CVE-2022-49035	https://git.kern el.org/stable/c/ 1609231f86760 c1f6a429de791 3dd795b9faa08 c, https://git.kern el.org/stable/c/ 2654e785bd4aa 2439cdffbe7dc1 ea30a0eddbfe4, https://git.kern el.org/stable/c/ 4a449430ecfb1 99b99ba58af63 c467eb53500b3	O-LIN-LINU- 200125/979
Affected Vers	ion(s): From (inc	cluding) 5.	5 Up to (excluding) 5.10.231		
Missing Release of Memory after Effective Lifetime	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix nfs4_openowner leak when concurrent nfsd4_open occur The action force umount(umount -f) will attempt to kill all rpc_task even umount operation may	https://git.kern el.org/stable/c/ 0ab0a3ad24e97 0e894abcac58f8 5c332d1726749 , https://git.kern el.org/stable/c/ 2d505a801e574 28057563762f6 7a5a62009b260 0, https://git.kern	O-LIN-LINU- 200125/980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ultimately fail if some files remain open. Consequently, if an action attempts to open a file, it can potentially send two rpc_task to nfs server.	el.org/stable/c/ 37dfc81266d3a 32294524bfadd 3396614f8633e e	
			NFS CLIENT thread1 thread2 open("file") nfs4_do_open _nfs4_do_open _nfs4_open_and_get_state		
			_nfs4_proc_open nfs4_run_open_task /* rpc_task1 */ rpc_run_task		
			rpc_wait_for_completion_tas k umount -		
			f		
			nfs_umount_begin		
			rpc_killall_tasks rpc_signal_task rpc_task1 been wakeup and return -512 _nfs4_do_open // while loop		
			 nfs4_run_open_task /* rpc_task2 */ rpc_run_task		
			rpc_wait_for_completion_tas		
			While processing an open request, nfsd will first attempt to find or allocate an nfs4_openowner. If it finds an nfs4_openowner that is not		
			marked as		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NFS4_OO_CONFIRMED, this nfs4_openowner will released. Since two rpc_task can attempt to open the same file simultaneously from the client to server, and because two instances of nfsd can run concurrently, this situation can lead to lots of memory leak. Additionally, when we echo 0 to /proc/fs/nfsd/threads, warning will be triggered.		
			NFS SERVER nfsd1 nfsd2 echo 0 > /proc/fs/nfsd/threads nfsd4_open		
			nfsd4_process_open1 find_or_alloc_open_stateow ner // alloc oo1, stateid1		
			nfsd4_process_open1 find_or_alloc_open_stateow ner		
			release_openowner unhash_openowner_locked list_del_init(&oo- >oo_perclient)		
			// cannot find this oo // from client, LEAK!!! alloc_stateowner // alloc oo2		

0-1

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nfsd4_process_open2 init_open_stateid // associate oo1 // with stateid1, stateid1 LEAK!!! nfs4_get_vfs_file // alloc nfsd_file1 and nfsd_file_mark1 // all LEAK!!!		
			nfsd4_process_open2 		
			write_threads 		
			nfsd_destroy_serv		
			nfsd_shutdown_net		
			nfs4_state_shutdown_net		
			nfs4_state_destroy_net		
			destroy_client		
			_destroy_client // won't find oo1!!!		
			nfsd_shutdown_generic		
			nfsd_file_cache_shutdown		
			kmem_cache_destroy for nfsd_file_slab		
			and nfsd_file_mark_slab		
			// bark since nfsd_file1		
			// and nfsd_file_mark1 // still alive		
			=======================================		
			=======================================		
			=======================================		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BUG nfsd_file (Not tainted): Objects remaining in nfsd_file on _kmem_cache_shutdown()		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: powerpc/prom_init: Fixup missing powermac #sizecells On some powermacs `escc` nodes are missing `#sizecells` properties, which is deprecated and now triggers a warning at boot since commit 045b14ca5c36 ("of: WARN on deprecated #addresscells/#size-cells handling"). For example: Missing '#size-cells' in /pci@f2000000/macio@c/escc@13000 WARNING: CPU: 0 PID: 0 at	https://git.kern el.org/stable/c/ 0b94d838018fb 0a824e0cd3149 034928c99fb1b 7, https://git.kern el.org/stable/c/ 296a109fa7711 0ba5267fe0e90 a26005eecc272 6, https://git.kern el.org/stable/c/ 691284c2cd33ff aa0b35ce53b32 86b90621e9dc9	O-LIN-LINU- 200125/981

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drivers/of/base.c:133 of_bus_n_size_cells+0x98/0 x108 Hardware name: PowerMac3,1 7400 0xc0209 PowerMac		
			Call Trace: of_bus_n_size_cells+0x98/0 x108 (unreliable)		
			of_bus_default_count_cells+ 0x40/0x60		
			_of_get_address+0xc8/0x2 1c		
			of_address_to_resource+0 x5c/0x228		
			pmz_init_port+0x5c/0x2ec pmz_probe.isra.0+0x144/0x		
			1e4 pmz_console_init+0x10/0x4		
			8 console_init+0xcc/0x138		
			start_kernel+0x5c4/0x694 As powermacs boot via		
			prom_init it's possible to add the missing properties to the device tree during boot, avoiding the warning. Note that `escc-legacy` nodes are also missing `#size-cells` properties, but they are skipped by the macio driver, so leave them alone.		
			Depends-on: 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling")		
			CVE ID: CVE-2024-56781		

CVSSv3 Scoring Scale
* stands for all versions 2-3 3-4 8-9 0-1 4-5 5-6 6-7 7-8 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): From (in	cluding) 5	5 Up to (excluding) 5.10.232		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sched: netem: account for backlog updates from child qdisc In general, 'qlen' of any classful qdisc should keep track of the number of packets that the qdisc itself and all of its children holds. In case of netem, 'qlen' only accounts for the packets in its internal tfifo. When netem is used with a child qdisc, the child qdisc can use 'qdisc_tree_reduce_backlog' to inform its parent, netem, about created or dropped SKBs. This function updates 'qlen' and the backlog statistics of netem, but netem does not account for changes made by a child qdisc. 'qlen' then indicates the wrong number of packets in the tfifo. If a child qdisc creates new SKBs during enqueue and informs its parent about this, netem's 'qlen' value is increased. When netem dequeues the newly created SKBs from the child, the 'qlen' in netem is not updated. If 'qlen' reaches the configured sch->limit, the enqueue function stops working, even though the tfifo is not full. Reproduce the bug: Ensure that the sender machine has GSO enabled.	el.org/stable/c/	O-LIN-LINU- 200125/982

0-1

4-5

5-6

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Configure netem as root qdisc and tbf as its child on the outgoing interface of the machine as follows: \$ tc qdisc add dev <oif> root handle 1: netem delay 100ms limit 100 \$ tc qdisc add dev <oif> parent 1:0 tbf rate 50Mbit burst 1542 latency 50ms</oif></oif>		
			Send bulk TCP traffic out via this interface, e.g., by running an iPerf3 client on the machine. Check the qdisc statistics: \$ tc -s qdisc show dev <oif></oif>		
			Statistics after 10s of iPerf3 TCP test before the fix (note that netem's backlog > limit, netem stopped accepting packets): qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 2767766 bytes 1848 pkt (dropped 652, overlimits 0 requeues 0) backlog 4294528236b 1155p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 2767766 bytes 1848 pkt (dropped 327, overlimits 7601 requeues 0) backlog 0b 0p requeues 0		
			Statistics after the fix: qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 37766372 bytes 24974 pkt (dropped 9, overlimits 0 requeues 0) backlog 0b 0p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 37766372 bytes		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
T CUMICOS			24974 pkt (dropped 327, overlimits 96017 requeues 0) backlog 0b 0p requeues 0 tbf segments the GSO SKBs (tbf_segment) and updates the netem's 'qlen'. The interface fully stops transferring packets and "locks". In this case, the child qdisc and tfifo are empty, but 'qlen' indicates the tfifo is at its limit and no more packets are accepted. This patch adds a counter for the entries in the tfifo. Netem's 'qlen' is only decreased when a packet is returned by its dequeue function, and not during enqueuing into the child qdisc. External updates to 'qlen' are thus accounted for and only the behavior of the backlog statistics changes. As in other qdiscs, 'qlen' then keeps track of how many packets are held in netem and all of its children. As before, sch->limit remains as the maximum number of packets in the tfifo. The same applies to netem's backlog statistics. CVE ID: CVE-2024-56770		
Affected Vers	s <mark>ion(s): From (inc</mark>	cluding) 6.	1.112 Up to (excluding) 6.1.	120	
Reachable Assertion	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_socket: remove WARN_ON_ONCE on maximum cgroup level cgroup maximum depth is	https://git.kern el.org/stable/c/ 2f9bec0a749eb6 46b384fde0c7b 7c24687b2ffae, https://git.kern el.org/stable/c/ 7064a6daa4a70 0a298fe3aee11d	0-LIN-LINU- 200125/983

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			INT_MAX by default, there is a cgroup toggle to restrict this maximum depth to a more reasonable value not to harm performance. Remove unnecessary WARN_ON_ONCE which is reachable from userspace. CVE ID: CVE-2024-56783	ea296bfe59fc4, https://git.kern el.org/stable/c/ b7529880cb961 d515642ce63f9 d7570869bbbdc 3	
Affected Vers	sion(s): From (in	cluding) 6.	1.120 Up to (excluding) 6.1.	123	
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free. CVE ID: CVE-2024-56766	https://git.kern el.org/stable/c/ 6ea15205d7e2b 811fbbdf79783f 686f58abfb4b7, https://git.kern el.org/stable/c/ d2f090ea57f8d6 587e09d4066f7 40a8617767b3d , https://git.kern el.org/stable/c/ d8e4771f99c04 00a1873235704 b28bb803c83d1 7	O-LIN-LINU- 200125/984
Affected Vers	sion(s): From (in	cluding) 6	1.53 Up to (excluding) 6.1.12	20	
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: quota: flush quota_release_work upon quota writeback One of the paths quota writeback is called from is: freeze_super() sync_filesystem() ext4_sync_fs() dquot_writeback_dquots() Since we currently don't always flush the	https://git.kern el.org/stable/c/ 3e6ff207cd5bd9 24ad94cd1a7c6 33bcdac0ba1cb, https://git.kern el.org/stable/c/ 6f3821acd7c31 4314599924808 7de5fb4b48cf26 , https://git.kern el.org/stable/c/ 8ea87e3479225 8825d290f4dc5 216276e91cb22 4	O-LIN-LINU- 200125/985

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			quota_release_work queue in this path, we can end up with the following race:		
			1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state:		
			ext4_journal_check_start+0x 28/0x110 [ext4] (unreliable)		
			_ext4_journal_start_sb+0x6 4/0x1c0 [ext4]		
			ext4_release_dquot+0x90/0 x1d0 [ext4]		
			quota_release_workfn+0x43 c/0x4d0		
			Which is the following line:		
			WARN_ON(sb- >s_writers.frozen == SB_FREEZE_COMPLETE);		
			Which ultimately results in generic/390 failing due to dmesg noise. This was detected on powerpc machine 15 cores.		
			To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze.		

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			CVE ID: CVE-2024-56780						
Affected Version(s): From (including) 6.1.54 Up to (excluding) 6.2									
NULL Pointer Dereference	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: check folio mapping after unlock in relocate_one_folio() When we call btrfs_read_folio() to bring a folio uptodate, we unlock the folio. The result of that is that a different thread can modify the mapping (like remove it with invalidate) before we call folio_lock(). This results in an invalid page and we need to try again. In particular, if we are relocating concurrently with aborting a transaction, this can result in a crash like the following: BUG: kernel NULL pointer dereference, address: 00000000000000000000000000000000000	https://git.kern el.org/stable/c/ 3e74859ee35ed c33a022c3f397 1df066ea0ca6b9 , https://git.kern el.org/stable/c/ d508e56270389 b3a16f5b3cf247 f4eb1bbad1578	O-LIN-LINU- 200125/986				

4-5

5-6

6-7

3-4

2-3

8-9

9-10

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x120		
			relocate_block_group+0x20f /0x480		
			btrfs_relocate_block_group+ 0x152/0x320		
			btrfs_relocate_chunk+0x3d/ 0x120		
			btrfs_reclaim_bgs_work+0x 2ae/0x4e0		
			process_scheduled_works+ 0x184/0x370		
			worker_thread+0xc6/0x3e0 ? blk_add_timer+0xb0/0xb0		
			kthread+0xae/0xe0		
			flush_tlb_kernel_range+0x9 0/0x90 ret_from_fork+0x2f/0x40		
			? flush_tlb_kernel_range+0x9 0/0x90		
			ret_from_fork_asm+0x11/0 x20 		
			This occurs because cleanup_one_transaction() calls		
			destroy_delalloc_inodes() which calls invalidate_inode_pages2()		
			which takes the folio_lock before		
			setting mapping to NULL. We fail to check		
			this, and subsequently call set_extent_mapping(), which assumes that		
			mapping != NULL (in fact it asserts that in debug mode)		
			Note that the "fixes" patch here is not the one that		
			introduced the		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): From (inc	cluding) 6	race (the very first iteration of this code from 2009) but a more recent change that made this particular crash happen in practice. CVE ID: CVE-2024-56758 10 Up to (excluding) 6.12.8		
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix bpf_get_smp_processor_id() on !CONFIG_SMP On x86-64 calling bpf_get_smp_processor_id() in a kernel with CONFIG_SMP disabled can trigger the following bug, as pcpu_hot is unavailable: [8.471774] BUG: unable to handle page fault for address: 00000000936a290c [8.471849] #PF: supervisor read access in kernel mode [8.471881] #PF: error_code(0x0000) - not-present page Fix by inlining a return 0 in the !CONFIG_SMP case. CVE ID: CVE-2024-56768	https://git.kern el.org/stable/c/ 23579010cf0a1 2476e96a5f1acd f78a9c5843657, https://git.kern el.org/stable/c/f 4ab7d74247b01 50547cf909b3f6 f24ee85183df	O-LIN-LINU- 200125/987
Affected Ver	sion(s): From (in	cluding) 6.	10.12 Up to (excluding) 6.12	2.5	
Reachable Assertion	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_socket: remove WARN_ON_ONCE on maximum cgroup level cgroup maximum depth is	https://git.kern el.org/stable/c/ 2f9bec0a749eb6 46b384fde0c7b 7c24687b2ffae, https://git.kern el.org/stable/c/ 7064a6daa4a70 0a298fe3aee11d	O-LIN-LINU- 200125/988

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			INT_MAX by default, there is a cgroup toggle to restrict this maximum depth to a more reasonable value not to harm performance. Remove unnecessary WARN_ON_ONCE which is reachable from userspace. CVE ID: CVE-2024-56783	ea296bfe59fc4, https://git.kern el.org/stable/c/ b7529880cb961 d515642ce63f9 d7570869bbbdc 3	
Affected Vers	sion(s): From (inc	cluding) 6.	11.11 Up to (excluding) 6.12		
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free. CVE ID: CVE-2024-56766	https://git.kern el.org/stable/c/ 6ea15205d7e2b 811fbbdf79783f 686f58abfb4b7, https://git.kern el.org/stable/c/ d2f090ea57f8d6 587e09d4066f7 40a8617767b3d , https://git.kern el.org/stable/c/ d8e4771f99c04 00a1873235704 b28bb803c83d1 7	O-LIN-LINU- 200125/989
Affected Vers	sion(s): From (in	cluding) 6.	12.2 Up to (excluding) 6.12.5	3	
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free. CVE ID: CVE-2024-56766	https://git.kern el.org/stable/c/ 6ea15205d7e2b 811fbbdf79783f 686f58abfb4b7, https://git.kern el.org/stable/c/ d2f090ea57f8d6 587e09d4066f7 40a8617767b3d , https://git.kern el.org/stable/c/ d8e4771f99c04 00a1873235704 b28bb803c83d1 7	O-LIN-LINU- 200125/990
Affected Vers	sion(s): From (inc	cluding) 6.	2 Up to (excluding) 6.6.64		

Γ	CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
	U										

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix nfs4_openowner leak when concurrent nfsd4_open occur The action force umount(umount -f) will attempt to kill all rpc_task even umount operation may ultimately fail if some files remain open. Consequently, if an action attempts to open a file, it can potentially send two rpc_task to nfs server. NFS CLIENT thread1 thread2 open("file") nfs4_do_opennfs4_do_opennfs4_open_and_get_statenfs4_proc_open nfs4_run_open_task /* rpc_task1 */ rpc_run_task rpc_wait_for_completion_tas k rpc_signal_task rpc_signal_task rpc_task1 been wakeup and return -512nfs4_do_open // while loop nfs4_run_open_task /* rpc_task2 */ rpc_task2 */	https://git.kern el.org/stable/c/ 0ab0a3ad24e97 0e894abcac58f8 5c332d1726749 , https://git.kern el.org/stable/c/ 2d505a801e574 28057563762f6 7a5a62009b260 0, https://git.kern el.org/stable/c/ 37dfc81266d3a 32294524bfadd 3396614f8633e e	O-LIN-LINU- 200125/991

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

	_		NCIIPC ID
	rpc_run_task rpc_wait_for_completion_tas k		
	While processing an open request, nfsd will first attempt to find or allocate an nfs4_openowner. If it finds an nfs4_openowner that is not marked as NFS4_OO_CONFIRMED, this		
	nfs4_openowner will released. Since two rpc_task can attempt to open the same file simultaneously from the client to server, and because two instances of nfsd can run concurrently, this situation can lead to lots of memory leak. Additionally, when we echo 0 to /proc/fs/nfsd/threads, warning will be		
	triggered. NFS SERVER nfsd1 nfsd2 echo 0 > /proc/fs/nfsd/threads nfsd4_open		
	find_or_alloc_open_stateow ner // alloc oo1, stateid1 nfsd4_open		
	nfsd4_process_open1 find_or_alloc_open_stateow ner		
		While processing an open request, nfsd will first attempt to find or allocate an nfs4_openowner. If it finds an nfs4_openowner that is not marked as NFS4_OO_CONFIRMED, this nfs4_openowner will released. Since two rpc_task can attempt to open the same file simultaneously from the client to server, and because two instances of nfsd can run concurrently, this situation can lead to lots of memory leak. Additionally, when we echo 0 to /proc/fs/nfsd/threads, warning will be triggered. NFS SERVER nfsd1 nfsd2 echo 0 > /proc/fs/nfsd/threads nfsd4_open nfsd4_process_open1 find_or_alloc_open_stateow ner // alloc oo1, stateid1 nfsd4_open nfsd4_process_open1 find_or_alloc_open_stateow ner // find oo1, without	While processing an open request, nfsd will first attempt to find or allocate an nfs4_openowner. If it finds an nfs4_openowner that is not marked as NFS4_OPENOWNER will released. Since two rpc_task can attempt to open the same file simultaneously from the client to server, and because two instances of nfsd can run concurrently, this situation can lead to lots of memory leak. Additionally, when we echo 0 to /proc/fs/nfsd/threads, warning will be triggered. NFS SERVER nfsd1 mfsd2 echo 0 > /proc/fs/nfsd/threads nfsd4_open nfsd4_open nfsd4_process_open1 find_or_alloc_open_stateow ner // alloc oo1, stateid1 nfsd4_open nfsd4_process_open1 find_or_alloc_open_stateow ner // find_oo1, without NFS4_OO_CONFIRMED

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unhash_openowner_locked		
			list_del_init(&oo- >oo_perclient)		
			alloc_stateowner // alloc oo2		
			nfsd4_process_open2 init_open_stateid // associate oo1 // with stateid1, stateid1 LEAK!!! nfs4_get_vfs_file // alloc nfsd_file1 and nfsd_file_mark1 // all LEAK!!!		
			nfsd4_process_open2 		
			write_threads 		
			nfsd_destroy_serv		
			nfsd_shutdown_net		
			nfs4_state_shutdown_net		
			nfs4_state_destroy_net		
			destroy_client		
			_destroy_client // won't find oo1!!!		
			nfsd_shutdown_generic		
			nfsd_file_cache_shutdown		
			kmem_cache_destroy for		
			nfsd_file_slab		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and nfsd_file_mark_slab // bark since nfsd_file1 // and nfsd_file_mark1 // still alive ===================================		
			CVE ID: CVE-2024-56779		
NULL Pointer Dereference	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: add a sanity check for btrfs root in btrfs_search_slot() Syzbot reports a null-ptr-deref in btrfs_search_slot(). The reproducer is using	https://git.kern el.org/stable/c/ 3ed51857a50f5 30ac7a1482e06 9dfbd1298558d 4, https://git.kern el.org/stable/c/ 757171d1369b3 b47f36932d40a 05a0715496dca b,	O-LIN-LINU- 200125/992

CVSSv3 Scoring Scale
* stands for all versions 3-4 8-9 9-10 0-1 2-3 4-5 5-6 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rescue=ibadroots, and the extent tree root is corrupted thus the extent tree is NULL. When scrub tries to search the extent tree to gather the needed extent info, btrfs_search_slot() doesn't check if the target root is NULL or not, resulting the null-ptr-deref.	https://git.kern el.org/stable/c/ 93992c3d9629b 02dccf6849238 559d5c24f2dece	
			Add sanity check for btrfs root before using it in btrfs_search_slot().		
			CVE ID: CVE-2024-56774		
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. CVE ID: CVE-2024-56776	https://git.kern el.org/stable/c/ 40725c5fabee80 4fecce41d4d5c5 bae80c45e1c4, https://git.kern el.org/stable/c/ 831214f77037d e02afc287eae93 ce97f218d8c04, https://git.kern el.org/stable/c/ 8ab73ac97c0fa5 28f66eeccd9bb5 3eb6eb7d20dc	O-LIN-LINU- 200125/993
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers in sti_hqvdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case	https://git.kern el.org/stable/c/ 31c857e7496d3 4e5a32a6f75bc0 24d0b06fd646a, https://git.kern el.org/stable/c/ 6b0d0d6e9d3c2 6697230bf7dc9 e6b52bdb24086 f, https://git.kern el.org/stable/c/ 82a5312f874fb1 8f045d9658e9b	O-LIN-LINU- 200125/994

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the failure.	d290e3b0621c0	
			CVE ID: CVE-2024-56778		
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers in sti_gdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. CVE ID: CVE-2024-56777	https://git.kern el.org/stable/c/ 3cf2e7c448e246 f7e700c7aa4745 0d1e27579559, https://git.kern el.org/stable/c/ 997b64c3f4c18 27c5cfda8ae7f5 d13f78d28b541, https://git.kern el.org/stable/c/ b79612ed6bc1a 184c45427105c 851b5b2d4342c a	0-LIN-LINU- 200125/995
Affected Vers	sion(s): From (inc	cluding) 6.	2 Up to (excluding) 6.6.66		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: powerpc/prom_init: Fixup missing powermac #sizecells On some powermacs 'escc' nodes are missing '#sizecells' properties, which is deprecated and now triggers a warning at boot since commit 045b14ca5c36 ("of: WARN on deprecated #addresscells/#size-cells handling"). For example: Missing '#size-cells' in /pci@f2000000/macio@c/escc@13000 WARNING: CPU: 0 PID: 0 at drivers/of/base.c:133 of_bus_n_size_cells+0x98/0x108 Hardware name:	https://git.kern el.org/stable/c/ 0b94d838018fb 0a824e0cd3149 034928c99fb1b 7, https://git.kern el.org/stable/c/ 296a109fa7711 0ba5267fe0e90 a26005eecc272 6, https://git.kern el.org/stable/c/ 691284c2cd33ff aa0b35ce53b32 86b90621e9dc9	O-LIN-LINU- 200125/996

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PowerMac3,1 7400 0xc0209 PowerMac		
			 Call Trace:		
			of_bus_n_size_cells+0x98/0 x108 (unreliable)		
			of_bus_default_count_cells+ 0x40/0x60		
			_of_get_address+0xc8/0x2 1c		
			_of_address_to_resource+0 x5c/0x228		
			pmz_init_port+0x5c/0x2ec		
			pmz_probe.isra.0+0x144/0x 1e4		
			pmz_console_init+0x10/0x4 8		
			console_init+0xcc/0x138		
			start_kernel+0x5c4/0x694		
			As powermacs boot via prom_init it's possible to add the missing properties to the device tree during boot, avoiding the warning. Note that `escc-legacy` nodes are also missing `#size-cells` properties, but they are skipped by the macio driver, so leave them alone.		
			Depends-on: 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling")		
			CVE ID: CVE-2024-56781		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kern el.org/stable/c/ 01575f2ff8ba57 8a3436f230668	O-LIN-LINU- 200125/997

CVSSv3 Scoring Scale
* stands for all versions 3-4 8-9 9-10 0-1 2-3 4-5 5-6 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MIPS: Loongson64: DTS: Really fix PCIe port nodes for ls7a Fix the dtc warnings: arch/mips/boot/dts/loongs on/ls7a-pch.dtsi:68.16- 416.5: Warning (interrupt_provider):	bd056dc2eb823 , https://git.kern el.org/stable/c/ 4fbd66d8254ce dfd1218393f39 d83b6c07a0191 7, https://git.kern el.org/stable/c/ 5a2eaa3ad2b80	
			/bus@10000000/pci@1a0 00000: '#interrupt-cells' found, but node is not an interrupt provider arch/mips/boot/dts/loongs	3c7ea442c6db7 379466ee73c02 4	
			on/ls7a-pch.dtsi:68.16- 416.5: Warning (interrupt_provider): /bus@10000000/pci@1a0 00000: '#interrupt-cells' found, but node is not an interrupt provider		
			arch/mips/boot/dts/loongs on/loongson64g_4core_ls7a .dtb: Warning (interrupt_map): Failed prerequisite 'interrupt_provider'		
			And a runtime warning introduced in commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"):		
			WARNING: CPU: 0 PID: 1 at drivers/of/base.c:106 of_bus_n_addr_cells+0x9c/0 xe0 Missing '#address-cells' in /bus@10000000/pci@1a0		
			00000/pci_bridge@9,0 The fix is similar to commit d89a415ff8d5 ("MIPS: Loongson64: DTS: Fix PCIe port nodes for ls7a"), which		

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has fixed the issue for ls2k (despite its subject mentions ls7a). CVE ID: CVE-2024-56785		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: soc: imx8m: Probe the SoC driver as platform driver With driver_async_probe=* on kernel command line, the following trace is produced because on i.MX8M Plus hardware because the soc-imx8m.c driver calls of_clk_get_by_name() which returns - EPROBE_DEFER because the clock driver is not yet probed. This was not detected during regular testing without driver_async_probe. Convert the SoC code to platform driver and instantiate a platform device in its current device_initcall() to probe the platform driver. Rework .soc_revision callback to always return valid error code and return SoC revision via parameter. This way, if anything in the .soc_revision callback return -EPROBE_DEFER, it gets propagated to .probe and the .probe will get retried later. "	https://git.kern el.org/stable/c/ 2129f6faa5dfe8 c6b87aad11720 bf75edd77d3e4, https://git.kern el.org/stable/c/ 997a3c04d7fa3 d1d385c146913 50d096fada648 c, https://git.kern el.org/stable/c/ 9cc832d37799d bea950c4c8a34 721b02b8b5a8ff	O-LIN-LINU- 200125/998

^{*} stands for all versions

drivers/soc/imx/soc- imx8m.c:115 imx8mm_soc_revision+0xdc /0x180 CPU: 1 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.11.0-next-20240924- 00002-g2062bb554dea #603 Hardware name: DH electronics i.MX8M Plus DHCOM Premium Developer Kit (3) (DT) pstate: 20000005 (nzCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=) pc : imx8mm_soc_revision+0xdc /0x180 lr : imx8mm_soc_revision+0xd 0/0x180 sp : ffff8000821fbcc0 x29: ffff8000821fbcc0 x29: ffff8000821fbcc0 x29: ffff8000821fbcc0 x29: ffff8000821fbcc0 x27: ffff800081810120
x26: ffff8000818a9970 x25: 000000000000000006 x24: 0000000000824311 x23: ffff8000817f42c8 x22: ffff0000df8be210 x21: fffffffffffffffdb x20: ffff800082780000 x19: 00000000000000001 x18: ffffffffffffffffffffffffffffffffffff

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	ffffffffffffffffb Call trace: imx8mm_soc_revision+0xdc /0x180 imx8_soc_init+0xb0/0x1e0 do_one_initcall+0x94/0x1a 8 kernel_init_freeable+0x240 /0x2a8 kernel_init+0x28/0x140 ret_from_fork+0x10/0x20	Patch	NCIIPC ID
Affacted Vov	pion(a), Erom (in	aluding) 6	[end trace 000000000000000000000000000000000000		
Affected vers		Juding) o	In the Linux kernel, the		
N/A	08-Jan-2025	5.5	following vulnerability has been resolved: net/sched: netem: account for backlog updates from child qdisc In general, 'qlen' of any classful qdisc should keep track of the number of packets that the qdisc itself and all of its children holds. In case of netem, 'qlen' only accounts for the packets in its internal tfifo. When netem is used with a child qdisc, the child qdisc can use 'qdisc_tree_reduce_backlog' to inform its parent, netem, about created or dropped SKBs. This function updates 'qlen' and the backlog statistics of netem, but netem does not account for changes made by a child qdisc. 'qlen' then indicates the	https://git.kern el.org/stable/c/ 10df49cfca73df bbdb6c4150d85 9f7e8926ae427, https://git.kern el.org/stable/c/ 216509dda290f 6db92c816dd54 b83c1df9da9e7 6, https://git.kern el.org/stable/c/ 356078a5c55ec 8d2061fcc009fb 8599f5b0527f9	O-LIN-LINU- 200125/999

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wrong number of packets in the tfifo. If a child qdisc creates new SKBs during enqueue and informs its parent about this, netem's 'qlen' value is increased. When netem dequeues the newly created SKBs from the child, the 'qlen' in netem is not updated. If 'qlen' reaches the configured sch->limit, the enqueue function stops working, even though the tfifo is not full.		
			Reproduce the bug: Ensure that the sender machine has GSO enabled. Configure netem as root qdisc and tbf as its child on the outgoing interface of the machine as follows: \$ tc qdisc add dev <oif> root handle 1: netem delay 100ms limit 100 \$ tc qdisc add dev <oif> parent 1:0 tbf rate 50Mbit burst 1542 latency 50ms</oif></oif>		
			Send bulk TCP traffic out via this interface, e.g., by running an iPerf3 client on the machine. Check the qdisc statistics: \$ tc -s qdisc show dev <oif></oif>		
			Statistics after 10s of iPerf3 TCP test before the fix (note that netem's backlog > limit, netem stopped accepting packets): qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 2767766 bytes 1848 pkt (dropped 652, overlimits 0 requeues 0) backlog 4294528236b 1155p requeues 0		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 2767766 bytes 1848 pkt (dropped 327, overlimits 7601 requeues 0) backlog 0b 0p requeues 0 Statistics after the fix: qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 37766372 bytes 24974 pkt (dropped 9, overlimits 0 requeues 0) backlog 0b 0p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 37766372 bytes 24974 pkt (dropped 327, overlimits 96017 requeues 0) backlog 0b 0p requeues 0 tbf segments the GSO SKBs (tbf_segment) and updates the netem's 'qlen'. The interface fully stops transferring packets and "locks". In this case, the child qdisc and tfifo are empty, but 'qlen' indicates	Patch	NCIIPC ID
			the tfifo is at its limit and no more packets are accepted. This patch adds a counter for the entries in the tfifo. Netem's 'qlen' is only decreased when a packet is returned by its dequeue function, and not during enqueuing into the child qdisc. External updates to 'qlen' are thus accounted for and only the behavior of the backlog statistics changes. As in other qdiscs, 'qlen' then keeps track of how many packets are held in		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s). From (in	cluding) 6	netem and all of its children. As before, sch->limit remains as the maximum number of packets in the tfifo. The same applies to netem's backlog statistics. CVE ID: CVE-2024-56770		
Use After Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries/vas: Add close() callback in vas_vm_ops struct The mapping VMA address is saved in VAS window struct when the paste address is mapped. This VMA address is used during migration to unmap the paste address if the window is active. The paste address mapping will be removed when the window is closed or with the munmap(). But the VMA address in the VAS window is not updated with munmap() which is causing invalid access during migration. The KASAN report shows: [16386.254991] BUG: KASAN: slab-use-after-free in reconfig_close_windows+0x 1a0/0x4e8 [16386.255043] Read of size 8 at addr c00000014a819670 by task drmgr/696928 [16386.255096] CPU: 29 UID: 0 PID: 696928 Comm: drmgr Kdump: loaded	https://git.kern el.org/stable/c/ 05aa156e156ef 3168e7ab8a687 21945196495c1 7, https://git.kern el.org/stable/c/ 6d9cd27105459 f169993a4c5f21 6499a946dbf34, https://git.kern el.org/stable/c/ 8b2282b508452 1254a2cd9742a 3f4e1d5b77f843	O-LIN-LINU- 200125/1000

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Tainted: G B		
			" [16386.256136] Allocated by task 696554 on cpu 31 at 16377.277618s: [16386.256149] kasan_save_stack+0x34/0x 68		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	[16386.256163] kasan_save_track+0x34/0x 80 [16386.256175] kasan_save_alloc_info+0x58 /0x74 [16386.256196]kasan_slab_alloc+0xb8/0x dc [16386.256209] kmem_cache_alloc_noprof+ 0x200/0x3d0 [16386.256225] vm_area_alloc+0x44/0x150 [16386.256245] mmap_region+0x214/0x10 c4	Patch	NCIIPC ID
			[16386.256265] do_mmap+0x5fc/0x750 [16386.256277] vm_mmap_pgoff+0x14c/0x 24c [16386.256292] ksys_mmap_pgoff+0x20c/0 x348 [16386.256303] sys_mmap+0xd0/0x160		
			[16386.256350] Freed by task 0 on cpu 31 at 16386.204848s: [16386.256363] kasan_save_stack+0x34/0x 68 [16386.256374] kasan_save_track+0x34/0x 80 [16386.256384] kasan_save_free_info+0x64/		
			0x10c [16386.256396] _kasan_slab_free+0x120/0 x204 [16386.256415] kmem_cache_free+0x128/0 x450 [16386.256428] vm_area_free_rcu_cb+0xa8/ 0xd8 [16386.256441] rcu_do_batch+0x2c8/0xcf0		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[16386.256458] rcu_core+0x378/0x3c4 [16386.256473] handle_softirqs+0x20c/0x6 0c [16386.256495] do_softirq_own_stack+0x6c /0x88 [16386.256509] do_softirq_own_stack+0x58 /0x88 [16386.256521]irq_exit_rcu+0x1a4/0x20c [16386.256533] irq_exit+0x20/0x38 [16386.256544] interrupt_async_exit_prepar e.constprop.0+0x18/0x2c		
			[16386.256717] Last potentially related work creation: [16386.256729] kasan_save_stack+0x34/0x 68 [16386.256741]kasan_record_aux_stack+0 xcc/0x12c [16386.256753]call_rcu_common.constpro p.0+0x94/0xd04 [16386.256766] vm_area_free+0x28/0x3c [16386.256778] remove_vma+0xf4/0x114 [16386.256797] do_vmi_align_munmap.cons tprop.0+0x684/0x870 [16386.256811]vm_munmap+0xe0/0x1f8 [16386.256821] sys_munmap+0x54/0x6c [16386.256830] system_call_exception+0x1a 0/0x4a0 [16386.256841] system_call_vectored_comm on+0x15c/0x2ec		
			[16386.256868] The buggy address belongs to the		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			object at c00000014a819670 which belongs to the cache vm_area_struct of size 168 [16386.256887] The buggy address is located 0 bytes inside of freed 168-byte region [c00000014a819670, c00000014a819718) [16386.256915] The buggy address belongs to the physical page: [16386.256928] page: refcount:1 mapcount:0 mapping:000000000000000000000000000000000000		
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: tracing: Prevent bad count for tracing_cpumask_write If a large count is provided, it will trigger a warning in bitmap_parse_user. Also check zero for it. CVE ID: CVE-2024-56763	https://git.kern el.org/stable/c/ 03041e474a6a8 f1bfd4b96b164 bb3165c48fa1a 3, https://git.kern el.org/stable/c/ 1cca920af19df5 dd91254e5ff35e 68e911683706, https://git.kern el.org/stable/c/ 3d15f4c244955 8ffe83b4dba306 14ef1cd6937c3	O-LIN-LINU- 200125/1001
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kern el.org/stable/c/ a60b990798eb1 7433d02837882	O-LIN-LINU- 200125/1002

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PCI/MSI: Handle lack of irqdomain gracefully	80422b1bd94b1 8,	
			Alexandre observed a warning emitted from pci_msi_setup_msi_irqs() on a RISCV platform which does not provide PCI/MSI support: WARNING: CPU: 1 PID: 1 at	https://git.kern el.org/stable/c/ aed157301c659 a48f5564cc456 8cf0e5c8831af0, https://git.kern el.org/stable/c/ b1f7476e07b93 d65a1a3643dcb 4a7bed80d4328	
			drivers/pci/msi/msi.h:121 pci_msi_setup_msi_irqs+0x2 c/0x32	d	
			pci_enable_msix_range+0x 30c/0x596		
			pci_msi_setup_msi_irqs+0x2 c/0x32		
			pci_alloc_irq_vectors_affinit y+0xb8/0xe2		
			RISCV uses hierarchical interrupt domains and correctly does not implement the legacy fallback. The warning triggers from the legacy fallback stub.		
			That warning is bogus as the PCI/MSI layer knows whether a PCI/MSI parent domain is associated with the device or not. There is a check for MSI-X, which has a legacy assumption. But that legacy fallback assumption is only valid when legacy support is enabled, but otherwise the check should simply return -ENOTSUPP.		
			Loongarch tripped over the same problem and blindly enabled legacy support without implementing the legacy fallbacks. There are		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			weak implementations which return an error, so the problem was papered over.		
			Correct pci_msi_domain_supports() to evaluate the legacy mode and add the missing supported check into the MSI enable path to complete it.		
			CVE ID: CVE-2024-56760		
			In the Linux kernel, the following vulnerability has been resolved:		
			media: dvb-frontends: dib3000mb: fix uninit-value in dib3000_write_reg		
			Syzbot reports [1] an uninitialized value issue found by KMSAN in dib3000_read_reg().	https://git.kern el.org/stable/c/ 1d6de21f00293	
Use of Uninitialized Resource	06-Jan-2025	5.5	Local u8 rb[2] is used in i2c_transfer() as a read buffer; in case that call fails, the buffer may end up with some undefined values.	d819b5ca6dbe7 5ff1f3b6392140, https://git.kern el.org/stable/c/ 2dd59fe0e19e1 ab95525997808 2b62e5751924c	O-LIN-LINU- 200125/1003
			Since no elaborate error handling is expected in dib3000_write_reg(), simply zero out rb buffer to mitigate the problem.	7, https://git.kern el.org/stable/c/ 3876e3a1c31a5 8a352c6bf5d2a 90e3304445a63	
			[1] Syzkaller report dvb-usb: bulk message failed: -22 (6/0)	7	
			=======================================		
			DUC VMCAN		
			BUG: KMSAN: uninit-value in dib3000mb_attach+0x2d8/ 0x3c0 drivers/media/dvb-		
			frontends/dib3000mb.c:75		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8 dib3000mb_attach+0x2d8/ 0x3c0 drivers/media/dvb- frontends/dib3000mb.c:75		
			dibusb_dib3000mb_fronten d_attach+0x155/0x2f0 drivers/media/usb/dvb- usb/dibusb-mb.c:31		
			dvb_usb_adapter_frontend_i nit+0xed/0x9a0 drivers/media/usb/dvb- usb/dvb-usb-dvb.c:290 dvb_usb_adapter_init drivers/media/usb/dvb- usb/dvb-usb-init.c:90 [inline] dvb_usb_init drivers/media/usb/dvb- usb/dvb-usb-init.c:186 [inline]		
			dvb_usb_device_init+0x25a 8/0x3760 drivers/media/usb/dvb- usb/dvb-usb-init.c:310 dibusb_probe+0x46/0x250 drivers/media/usb/dvb- usb/dibusb-mb.c:110 		
			Local variable rb created at: dib3000_read_reg+0x86/0x 4e0 drivers/media/dvb- frontends/dib3000mb.c:54		
			dib3000mb_attach+0x123/ 0x3c0 drivers/media/dvb- frontends/dib3000mb.c:75 8		
			CVE ID: CVE-2024-56769		
NULL Pointer Dereference	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kern el.org/stable/c/ 54376d8d2659 6f98ed7432a78	O-LIN-LINU- 200125/1004
			dmaengine: at_xdmac: avoid	8314bb9154bf3	

CVSSv3 Scoring Scale
* stands for all versions 3-4 8-9 9-10 0-1 2-3 4-5 5-6 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			null_prt_deref in at_xdmac_prep_dma_memse t The at_xdmac_memset_create_d esc may return NULL, which will lead to a null pointer dereference. For example, the len input is error, or the atchan->free_descs_list is empty and memory is exhausted. Therefore, add check to avoid this. CVE ID: CVE-2024-56767	e3, https://git.kern el.org/stable/c/ c43ec96e8d343 99bd9dab2f2dc 316b904892133 f, https://git.kern el.org/stable/c/ e658f1c133b85 4b2ae79914730 1d82dddb8f316 2	
Affected Ver	 <mark>sion(s): From (inc</mark>	cluding) 6	4.16 Up to (excluding) 6.5		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: quota: flush quota_release_work upon quota writeback One of the paths quota writeback is called from is: freeze_super() sync_filesystem() ext4_sync_fs() dquot_writeback_dquots() Since we currently don't always flush the quota_release_work queue in this path, we can end up with the following race: 1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to	https://git.kern el.org/stable/c/ 3e6ff207cd5bd9 24ad94cd1a7c6 33bcdac0ba1cb, https://git.kern el.org/stable/c/ 6f3821acd7c31 4314599924808 7de5fb4b48cf26 , https://git.kern el.org/stable/c/ 8ea87e3479225 8825d290f4dc5 216276e91cb22 4	O-LIN-LINU- 200125/1005

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state:		
			ext4_journal_check_start+0x 28/0x110 [ext4] (unreliable)		
			_ext4_journal_start_sb+0x6 4/0x1c0 [ext4]		
			ext4_release_dquot+0x90/0 x1d0 [ext4]		
			quota_release_workfn+0x43 c/0x4d0		
			Which is the following line:		
			WARN_ON(sb- >s_writers.frozen == SB_FREEZE_COMPLETE);		
			Which ultimately results in generic/390 failing due to dmesg noise. This was detected on powerpc machine 15 cores.		
			To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze.		
			CVE ID: CVE-2024-56780		
Affected Vers	sion(s): From (inc	cluding) 6.	5.3 Up to (excluding) 6.6.64		
			In the Linux kernel, the following vulnerability has been resolved:	https://git.kern el.org/stable/c/ 3e6ff207cd5bd9 24ad94cd1a7c6	o any any
N/A	08-Jan-2025	5.5	quota: flush quota_release_work upon quota writeback One of the paths quota	33bcdac0ba1cb, https://git.kern el.org/stable/c/ 6f3821acd7c31 4314599924808	O-LIN-LINU- 200125/1006
<u> </u>			writeback is called from is:	7de5fb4b48cf26	

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			freeze_super() sync_filesystem() ext4_sync_fs()	, https://git.kern el.org/stable/c/ 8ea87e3479225	
			dquot_writeback_dquots()	8825d290f4dc5 216276e91cb22	
			Since we currently don't always flush the quota_release_work queue in this path, we can end up with the following race:		
			1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state:		
			ext4_journal_check_start+0x 28/0x110 [ext4] (unreliable)		
			_ext4_journal_start_sb+0x6 4/0x1c0 [ext4]		
			ext4_release_dquot+0x90/0 x1d0 [ext4]		
			quota_release_workfn+0x43 c/0x4d0		
			Which is the following line:		
			WARN_ON(sb- >s_writers.frozen == SB_FREEZE_COMPLETE);		
			Which ultimately results in generic/390 failing due to dmesg		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			noise. This was detected on powerpc machine 15 cores. To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze. CVE ID: CVE-2024-56780		
Affected Vers	sion(s): From (in	cluding) 6	5.4 Up to (excluding) 6.12.8		
NULL Pointer Dereference	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: check folio mapping after unlock in relocate_one_folio() When we call btrfs_read_folio() to bring a folio uptodate, we unlock the folio. The result of that is that a different thread can modify the mapping (like remove it with invalidate) before we call folio_lock(). This results in an invalid page and we need to try again. In particular, if we are relocating concurrently with aborting a transaction, this can result in a crash like the following: BUG: kernel NULL pointer dereference, address: 00000000000000000000000000000000000	https://git.kern el.org/stable/c/ 3e74859ee35ed c33a022c3f397 1df066ea0ca6b9 , https://git.kern el.org/stable/c/ d508e56270389 b3a16f5b3cf247 f4eb1bbad1578	O-LIN-LINU- 200125/1007

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	0010:set_page_extent_mapp ed+0x20/0xb0 RSP: 0018:ffffc900516a7be8 EFLAGS: 00010246 RAX: ffffea009e851d08 RBX: ffffea009e0b1880 RCX: 000000000000000000000000000000000000	Patch	NCIIPC ID
			PKRU: 5555554 Call Trace: <task> ?die+0x78/0xc0 ? page_fault_oops+0x2a8/0x3 a0</task>		
			?switch_to+0x133/0x530 ? wq_worker_running+0xa/0 x40 ? exc_page_fault+0x63/0x130 ? asm_exc_page_fault+0x22/0		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x30		
			? set_page_extent_mapped+0		
			x20/0xb0		
			relocate_file_extent_cluster+		
			0x1a7/0x940		
			relocate_data_extent+0xaf/		
			0x120 '		
			relocate_block_group+0x20f		
			/0x480		
			btrfs_relocate_block_group+		
			0x152/0x320		
			btrfs_relocate_chunk+0x3d/		
			0x120		
			btrfs_reclaim_bgs_work+0x		
			2ae/0x4e0		
			process_scheduled_works+		
			0x184/0x370		
			worker_thread+0xc6/0x3e0		
			?		
			blk_add_timer+0xb0/0xb0 kthread+0xae/0xe0		
			?		
			flush_tlb_kernel_range+0x9 0/0x90		
			ret_from_fork+0x2f/0x40		
			? flush_tlb_kernel_range+0x9		
			0/0x90		
			ret_from_fork_asm+0x11/0		
			x20		
			This occurs because		
			cleanup_one_transaction() calls		
			destroy_delalloc_inodes()		
			which calls		
			invalidate_inode_pages2() which		
			takes the folio_lock before		
			setting mapping to NULL. We fail to check		

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this, and subsequently call set_extent_mapping(), which assumes that mapping != NULL (in fact it asserts that in debug mode)		
			Note that the "fixes" patch here is not the one that introduced the race (the very first iteration of this code from 2009) but a more recent change that made this particular crash happen in practice.		
			CVE ID: CVE-2024-56758		
Affected Vers	sion(s): From (inc	cluding) 6	6 Up to (excluding) 6.12.8		
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: x86/fred: Clear WFE in missing-ENDBRANCH #CPs An indirect branch instruction sets the CPU indirect branch tracker (IBT) into WAIT_FOR_ENDBRANCH (WFE) state and WFE stays asserted across the instruction boundary. When the decoder finds an inappropriate instruction while WFE is set ENDBR, the CPU raises a #CP fault.	https://git.kern el.org/stable/c/ b939f108e86b7 6119428a6fa4e 92491e09ac786 7, https://git.kern el.org/stable/c/ dc81e556f2a01 7d681251ace21 bf06c126d5a19	O-LIN-LINU- 200125/1008
			For the "kernel IBT no ENDBR" selftest where #CPs are deliberately triggered, the WFE state of the interrupted context needs to be cleared to let execution continue. Otherwise when the CPU resumes from the instruction that just caused the previous	2	

0-1

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			#CP, another missing-ENDBRANCH #CP is raised and the CPU enters a dead loop.		
			This is not a problem with IDT because it doesn't preserve WFE and IRET doesn't set WFE. But FRED provides space on the entry stack (in an expanded CS area) to save and restore the WFE state, thus the WFE state is no longer clobbered, so software must clear it.		
			Clear WFE to avoid dead looping in ibt_clear_fred_wfe() and the !ibt_fatal code path when execution is allowed to continue.		
			Clobbering WFE in any other circumstance is a security-relevant bug.		
			[dhansen: changelog rewording]		
			CVE ID: CVE-2024-56761		
Affected Vers	sion(s): From (inc	cluding) 6.	.6.53 Up to (excluding) 6.6.6	6	
			In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_socket: remove WARN_ON_ONCE on maximum cgroup level	https://git.kern el.org/stable/c/ 2f9bec0a749eb6 46b384fde0c7b 7c24687b2ffae, https://git.kern el.org/stable/c/	
Reachable Assertion	08-Jan-2025	5.5	cgroup maximum depth is INT_MAX by default, there is a cgroup toggle to restrict this maximum depth to a more reasonable value not to harm performance. Remove unnecessary WARN_ON_ONCE which is	7064a6daa4a70 0a298fe3aee11d ea296bfe59fc4, https://git.kern el.org/stable/c/ b7529880cb961 d515642ce63f9 d7570869bbbdc	0-LIN-LINU- 200125/1009

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			reachable from userspace.						
			CVE ID: CVE-2024-56783						
Affected Vers	Affected Version(s): From (including) 6.6.64 Up to (excluding) 6.6.69								
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free. CVE ID: CVE-2024-56766	https://git.kern el.org/stable/c/ 6ea15205d7e2b 811fbbdf79783f 686f58abfb4b7, https://git.kern el.org/stable/c/ d2f090ea57f8d6 587e09d4066f7 40a8617767b3d , https://git.kern el.org/stable/c/ d8e4771f99c04 00a1873235704 b28bb803c83d1	O-LIN-LINU- 200125/1010				
Affected Vers	sion(s): From (in	cluding) 6	7 Up to (excluding) 6.12.4	7					
Use After Free	08-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: kunit: string-stream: Fix a UAF bug in kunit_init_suite() In kunit_debugfs_create_suite(), if alloc_string_stream() fails in the kunit_suite_for_each_test_ca se() loop, the "suite->log = stream" has assigned before, and the error path only free the suite->log's stream memory but not set it to NULL, so the later string_stream_clear() of suite->log in kunit_init_suite() will cause below UAF bug. Set stream pointer to NULL after free to fix it.	https://git.kern el.org/stable/c/ 3213b92754b94 dec6836e8b4d6 ec7d224a805b6 1, https://git.kern el.org/stable/c/ 39e21403c9788 62846fa68b7f6d 06f9cca235194	O-LIN-LINU- 200125/1011				

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TT 11 . 1 . 1		
			Unable to handle		
			kernel paging request at virtual address		
			006440150000030d		
			Mem abort info:		
			ESR =		
			0x0000000096000004		
			EC = 0x25: DABT		
			(current EL), $IL = 32$ bits		
			SET = 0, FnV = 0		
			EA = 0, S1PTW = 0 $ESC = 0.004, love = 0$		
			FSC = 0x04: level 0 translation fault		
			Data abort info:		
			ISV = 0, ISS =		
			0×000000004 , ISS2 =		
			0x00000000		
			CM = 0, $WnR = 0$,		
			TnD = 0, $TagAccess = 0$		
			GCS = 0, Overlay =		
			0, DirtyBit = 0, $Xs = 0$		
			[006440150000030		
			d] address between user and kernel address ranges		
			Internal error:		
			Oops: 000000096000004		
			[#1] PREEMPT SMP		
			Dumping ftrace		
			buffer:		
			(ftrace buffer		
			empty)		
			Modules linked in:		
			iio_test_gts industrialio_gts_helper		
			cfg80211 rfkill ipv6 [last		
			unloaded: iio_test_gts]		
			CPU: 5 UID: 0 PID:		
			6253 Comm: modprobe		
			Tainted: G B W N		
			6.12.0-rc4+ #458		
			Tainted:		
			[B]=BAD_PAGE,		
			[W]=WARN, [N]=TEST Hardware name:		
			linux,dummy-virt (DT)		
			pstate: 40000005		
			(nZcv daif -PAN -UAO -TCO -		
			DIT -SSBS BTYPE=)		
			pc :		
			string_stream_clear+0x54/0		
			x1ac		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lr : string_stream_clear+0x1a8/ 0x1ac		
			x29: ffffffc080b47410 x28: 006440550000030d x27: ffffff80c96b5e98		
			x26: ffffff80c96b5e80 x25: ffffffe461b3f6c0 x24: 00000000000000003 x23:		
			ffffff80c96b5e88 x22: 1ffffff019cdf4fc x21: dfffffc000000000 x20:		
			ffffff80ce6fa7e0 x19: 032202a80000186d x18: 00000000000001840 x17:		
			0000000000000000 x16: 00000000000000000 x15: ffffffe45c355cb4 x14:		
			ffffffe45c35589c x13: ffffffe45c03da78 x12: ffffffb810168e75 x11:		
			1ffffff810168e74 x10: ffffffb810168e74 x9 : dfffffc000000000 x8 :		
			00000000000000004 x7 : 000000000000000003 x6 : 00000000000000001 x5 :		
			ffffffc080b473a0 x4 : 000000000000000000000000000000000		
			0000000000000001 x1 : ffffffe462fbf620 x0 : dfffffc000000000 Call trace:		
			string_stream_clear+0x54/0 x1ac		
			_kunit_test_suites_init+0x1 08/0x1d8		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kunit_exec_run_tests+0xb8/ 0x100		
			kunit_module_notify+0x400 /0x55c		
			notifier_call_chain+0xfc/0x 3b4		
			blocking_notifier_call_chain +0x68/0x9c		
			do_init_module+0x24c/0x5 c8		
			load_module+0x4acc/0x4e9 0		
			init_module_from_file+0xd4 /0x128		
			idempotent_init_module+0x 2d4/0x57c		
			_arm64_sys_finit_module+ 0xac/0x100		
			invoke_syscall+0x6c/0x258		
			el0_svc_common.constprop. 0+0x160/0x22c		
			do_el0_svc+0x44/0x5c el0_svc+0x48/0xb8		
			el0t_64_sync_handler+0x13 c/0x158		
			el0t_64_sync+0x190/0x194 Code: f9400753 d2dff800 f2fbffe0 d343fe7c (38e06b80)		
			[end trace 00000000000000000] Kernel panic - not		
			syncing: Oops: Fatal exception		
			CVE ID: CVE-2024-56772		
N/A	08-Jan-2025	5.5	In the Linux kernel, the	https://git.kern	O-LIN-LINU-

CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			following vulnerability has been resolved: mtd: spinand: winbond: Fix 512GW, 01GW, 01JW and 02JW ECC information These four chips: * W25N512GW * W25N01JW * W25N02JW all require a single bit of ECC strength and thus feature an on-die Hamming-like ECC engine. There is no point in filling a ->get_status() callback for them because the main ECC status bytes are located in standard places, and retrieving the number of bitflips in case of corrected chunk is both useless and unsupported (if there are bitflips, then there is 1 at most, so no need to query the chip for that). Without this change, a kernel warning triggers every time a bit flips. CVE ID: CVE-2024-56771	el.org/stable/c/ 234d5f75c3ae9 11b52c5e4442b 8a87fbbd12983 6, https://git.kern el.org/stable/c/f ee9b240916df8 2a8b07aef0fdfe 96785417a164	200125/1012
NULL Pointer Dereference	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: add a sanity check for btrfs root in btrfs_search_slot() Syzbot reports a null-ptr-deref in btrfs_search_slot(). The reproducer is using rescue=ibadroots, and the extent tree root is corrupted thus the extent	https://git.kern el.org/stable/c/ 3ed51857a50f5 30ac7a1482e06 9dfbd1298558d 4, https://git.kern el.org/stable/c/ 757171d1369b3 b47f36932d40a 05a0715496dca b, https://git.kern el.org/stable/c/ 93992c3d9629b	O-LIN-LINU- 200125/1013

CVSSv3 Scoring Scale
* stands for all versions 3-4 8-9 9-10 0-1 2-3 4-5 5-6 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tree is NULL. When scrub tries to search the extent tree to gather the needed extent info, btrfs_search_slot() doesn't check if the target root is NULL or not, resulting the null-ptr-deref. Add sanity check for btrfs root before using it in btrfs_search_slot(). CVE ID: CVE-2024-56774	02dccf6849238 559d5c24f2dece	
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers in sti_gdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. CVE ID: CVE-2024-56777	https://git.kern el.org/stable/c/ 3cf2e7c448e246 f7e700c7aa4745 0d1e27579559, https://git.kern el.org/stable/c/ 997b64c3f4c18 27c5cfda8ae7f5 d13f78d28b541, https://git.kern el.org/stable/c/ b79612ed6bc1a 184c45427105c 851b5b2d4342c a	O-LIN-LINU- 200125/1014
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. CVE ID: CVE-2024-56776	https://git.kern el.org/stable/c/ 40725c5fabee80 4fecce41d4d5c5 bae80c45e1c4, https://git.kern el.org/stable/c/ 831214f77037d e02afc287eae93 ce97f218d8c04, https://git.kern el.org/stable/c/ 8ab73ac97c0fa5 28f66eeccd9bb5 3eb6eb7d20dc	O-LIN-LINU- 200125/1015

5-6

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix nfs4_openowner leak when concurrent nfsd4_open occur The action force umount(umount -f) will attempt to kill all rpc_task even umount operation may ultimately fail if some files remain open. Consequently, if an action attempts to open a file, it can potentially send two rpc_task to nfs server. NFS CLIENT thread1 thread2 open("file") nfs4_do_opennfs4_do_opennfs4_open_and_get_statenfs4_proc_open nfs4_run_open_task /* rpc_task1 */ rpc_run_task rpc_wait_for_completion_tas k rpc_signal_task rpc_signal_task rpc_task1 been wakeup and return -512nfs4_do_open // while loop nfs4_run_open_task /* rpc_task2 */	https://git.kern el.org/stable/c/ 0ab0a3ad24e97 0e894abcac58f8 5c332d1726749 , https://git.kern el.org/stable/c/ 2d505a801e574 28057563762f6 7a5a62009b260 0, https://git.kern el.org/stable/c/ 37dfc81266d3a 32294524bfadd 3396614f8633e e	O-LIN-LINU- 200125/1016

0-1

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rpc_run_task		
			rpc_wait_for_completion_tas		
			k		
			While processing an open		
			request, nfsd will first attempt to find or		
			allocate an		
			nfs4_openowner. If it finds an nfs4_openowner that is		
			not		
			marked as NFS4_00_CONFIRMED, this		
			nfs4_openowner will		
			released. Since two rpc_task can attempt to		
			open the same file		
			simultaneously from the client to server, and because		
			two instances of nfsd can		
			run		
			concurrently, this situation can lead to lots of memory		
			leak.		
			Additionally, when we echo 0 to /proc/fs/nfsd/threads,		
			warning will be		
			triggered.		
			NFS SERVER		
			nfsd1 nfsd2 echo 0 >		
			/proc/fs/nfsd/threads		
			nfsd4_open		
			nfsd4_process_open1		
			find_or_alloc_open_stateow		
			ner		
			// alloc oo1, stateid1 nfsd4_open		
			_		
			nfsd4_process_open1		
			find_or_alloc_open_stateow		
			ner // find oo1,		
			without		
			NFS4_OO_CONFIRMED		
			release_openowner		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unhash_openowner_locked		
			list_del_init(&oo- >oo_perclient)		
			alloc_stateowner // alloc oo2		
			nfsd4_process_open2 init_open_stateid // associate oo1 // with stateid1, stateid1 LEAK!!! nfs4_get_vfs_file // alloc nfsd_file1 and nfsd_file_mark1 // all LEAK!!!		
			nfsd4_process_open2 		
			write_threads 		
			nfsd_destroy_serv		
			nfsd_shutdown_net		
			nfs4_state_shutdown_net		
			nfs4_state_destroy_net		
			destroy_client		
			_destroy_client // won't find oo1!!!		
			nfsd_shutdown_generic		
			nfsd_file_cache_shutdown		
			kmem_cache_destroy		
			for nfsd_file_slab		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and nfsd_file_mark_slab // bark since nfsd_file1 // and nfsd_file_mark1 // still alive ===================================		
			CVE ID: CVE-2024-56779		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: quota: flush quota_release_work upon quota writeback One of the paths quota writeback is called from is:	https://git.kern el.org/stable/c/ 3e6ff207cd5bd9 24ad94cd1a7c6 33bcdac0ba1cb, https://git.kern el.org/stable/c/ 6f3821acd7c31 4314599924808 7de5fb4b48cf26	O-LIN-LINU- 200125/1017

CVSSv3 Scoring Scale
* stands for all versions 3-4 8-9 9-10 0-1 2-3 4-5 5-6 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sync_filesystem() ext4_sync_fs()	el.org/stable/c/ 8ea87e3479225 8825d290f4dc5	
			dquot_writeback_dquots()	216276e91cb22	
			Since we currently don't always flush the quota_release_work queue in this path, we can end up with the following race:	7	
			1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state:		
			ext4_journal_check_start+0x 28/0x110 [ext4] (unreliable)		
			_ext4_journal_start_sb+0x6 4/0x1c0 [ext4]		
			ext4_release_dquot+0x90/0 x1d0 [ext4]		
			quota_release_workfn+0x43 c/0x4d0		
			Which is the following line:		
			WARN_ON(sb- >s_writers.frozen == SB_FREEZE_COMPLETE);		
			Which ultimately results in generic/390 failing due to dmesg noise. This was detected on powerpc machine 15 cores.		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze.		
			CVE ID: CVE-2024-56780		
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers in sti_hqvdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. CVE ID: CVE-2024-56778	https://git.kern el.org/stable/c/ 31c857e7496d3 4e5a32a6f75bc0 24d0b06fd646a, https://git.kern el.org/stable/c/ 6b0d0d6e9d3c2 6697230bf7dc9 e6b52bdb24086 f, https://git.kern el.org/stable/c/ 82a5312f874fb1 8f045d9658e9b d290e3b0621c0	O-LIN-LINU- 200125/1018
Affected Vers	sion(s): From (in	cluding) 6	7 Up to (excluding) 6.12.5		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: powerpc/prom_init: Fixup missing powermac #sizecells On some powermacs `escc` nodes are missing `#sizecells` properties, which is deprecated and now triggers a warning at boot since commit 045b14ca5c36 ("of: WARN on deprecated #addresscells/#size-cells handling"). For example: Missing '#size-cells' in /pci@f2000000/mac-	https://git.kern el.org/stable/c/ 0b94d838018fb 0a824e0cd3149 034928c99fb1b 7, https://git.kern el.org/stable/c/ 296a109fa7711 0ba5267fe0e90 a26005eecc272 6, https://git.kern el.org/stable/c/ 691284c2cd33ff aa0b35ce53b32 86b90621e9dc9	O-LIN-LINU- 200125/1019

5-6

6-7

7-8

9-10

3-4

Weakness	kness Publish Date CVSSv3 Desc		Description & CVE ID	Patch	NCIIPC ID
			io@c/escc@13000 WARNING: CPU: 0 PID: 0 at drivers/of/base.c:133 of_bus_n_size_cells+0x98/0 x108 Hardware name: PowerMac3,1 7400 0xc0209 PowerMac		
			 Call Trace:		
			of_bus_n_size_cells+0x98/0 x108 (unreliable)		
			of_bus_default_count_cells+ 0x40/0x60		
			_of_get_address+0xc8/0x2 1c		
			_of_address_to_resource+0 x5c/0x228		
			pmz_init_port+0x5c/0x2ec		
			pmz_probe.isra.0+0x144/0x 1e4		
			pmz_console_init+0x10/0x4 8 console_init+0xcc/0x138		
			start_kernel+0x5c4/0x694		
			As powermacs boot via prom_init it's possible to add the missing properties to the device tree during boot, avoiding the warning. Note that `escc-legacy` nodes are also missing `#size-cells` properties, but they are skipped by the macio driver, so leave them alone.		
			Depends-on: 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling")		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-56781		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: put bpf_link's program when link is safe to be deallocated In general, BPF link's underlying BPF program should be considered to be reachable through attach hook -> link -> prog chain, and, pessimistically, we have to assume that as long as link's memory is not safe to free, attach hook's code might hold a pointer to BPF program and use it. As such, it's not (generally) correct to put link's program early before waiting for RCU GPs to go through. More eager bpf_prog_put() that we currently do is mostly correct due to BPF program's release code doing similar RCU GP waiting, but as will be shown in the following patches, BPF program can be non-sleepable (and, thus, reliant on only "classic" RCU GP), while BPF link's attach hook can have sleepable semantics and needs to be protected by RCU Tasks Trace, and for such cases BPF link has to go through RCU Tasks Trace + "classic" RCU GPs before being deallocated. And so, if we put BPF program early, we might free BPF	https://git.kern el.org/stable/c/ 2fcb921c2799c4 9ac5e365cf4110 f94a64ae4885, https://git.kern el.org/stable/c/ 5fe23c57abadfd 46a7a66e81f35 36e4757252a0b , https://git.kern el.org/stable/c/f 44ec8733a8469 143fde1984b5e 6931b2e2f6f3f	O-LIN-LINU- 200125/1020

CVSSv3 Scoring Scale
* stands for all versions 0-1 2-3 3-4 4-5 5-6 6-7 7-8 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			program before we free BPF link, leading to use-after-free situation.		
			So, this patch defers bpf_prog_put() until we are ready to perform bpf_link's deallocation. At worst, this delays BPF program freeing by one extra RCU GP, but that seems completely acceptable. Alternatively, we'd need more elaborate ways to determine BPF hook, BPF link, and BPF program lifetimes, and how they relate to each other, which seems like an unnecessary complication.		
			Note, for most BPF links we still will perform eager bpf_prog_put() and link dealloc, so for those BPF links there are no observable changes whatsoever. Only BPF links that use deferred dealloc might notice slightly delayed freeing of BPF programs.		
			Also, to reduce code and logic duplication, extract program put + link dealloc logic into bpf_link_dealloc() helper.		
			CVE ID: CVE-2024-56786		
N/A	00 Ior 2025	F F	In the Linux kernel, the following vulnerability has been resolved: soc: imx8m: Probe the SoC	https://git.kern el.org/stable/c/ 2129f6faa5dfe8 c6b87aad11720 bf75edd77d3e4,	O-LIN-LINU-
N/A	08-Jan-2025	5.5	driver as platform driver With driver_async_probe=* on kernel command line, the following trace is	https://git.kern el.org/stable/c/ 997a3c04d7fa3 d1d385c146913 50d096fada648	200125/1021

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			produced because on i.MX8M Plus hardware because the soc-imx8m.c driver calls of_clk_get_by_name() which returns - EPROBE_DEFER because the clock driver is not yet probed. This was not detected during regular testing without driver_async_probe.	c, https://git.kern el.org/stable/c/ 9cc832d37799d bea950c4c8a34 721b02b8b5a8ff	
			Convert the SoC code to platform driver and instantiate a platform device in its current device_initcall() to probe the platform driver. Rework .soc_revision callback to always return valid error code and return SoC revision via parameter. This way, if anything in the .soc_revision callback return -EPROBE_DEFER, it gets propagated to .probe and the .probe will get retried later.		
			"		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pc : imx8mm_soc_revision+0xdc /0x180		
			Call trace: imx8mm_soc_revision+0xdc /0x180 imx8_soc_init+0xb0/0x1e0 do_one_initcall+0x94/0x1a 8 kernel_init_freeable+0x240 /0x2a8 kernel_init+0x28/0x140 ret_from_fork+0x10/0x20[end trace 000000000000000000000000000000000000		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SoC: i.MX8MP revision 1.1 " CVE ID: CVE-2024-56787		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: MIPS: Loongson64: DTS: Really fix PCIe port nodes for ls7a Fix the dtc warnings: arch/mips/boot/dts/loongs on/ls7a-pch.dtsi:68.16-416.5: Warning (interrupt_provider): /bus@10000000/pci@1a0 00000: '#interrupt-cells' found, but node is not an interrupt provider arch/mips/boot/dts/loongs on/ls7a-pch.dtsi:68.16-416.5: Warning (interrupt_provider): /bus@10000000/pci@1a0	https://git.kern el.org/stable/c/ 01575f2ff8ba57 8a3436f230668 bd056dc2eb823 , https://git.kern el.org/stable/c/ 4fbd66d8254ce dfd1218393f39	O-LIN-LINU- 200125/1022
IN/A			/bus@1000000/pci@1a0 00000: '#interrupt-cells' found, but node is not an interrupt provider arch/mips/boot/dts/loongs on/loongson64g_4core_ls7a .dtb: Warning (interrupt_map): Failed prerequisite 'interrupt_provider'	d83b6c07a0191 7, https://git.kern el.org/stable/c/ 5a2eaa3ad2b80 3c7ea442c6db7 379466ee73c02	
			And a runtime warning introduced in commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"): WARNING: CPU: 0 PID: 1 at drivers/of/base.c:106 of_bus_n_addr_cells+0x9c/0 xe0		

CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Missing '#address-cells' in /bus@10000000/pci@1a0 00000/pci_bridge@9,0 The fix is similar to commit d89a415ff8d5 ("MIPS: Loongson64: DTS: Fix PCIe port nodes for ls7a"), which has fixed the issue for ls2k (despite its subject mentions ls7a). CVE ID: CVE-2024-56785		
N/A	o8-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sched: netem: account for backlog updates from child qdisc In general, 'qlen' of any classful qdisc should keep track of the number of packets that the qdisc itself and all of its children holds. In case of netem, 'qlen' only accounts for the packets in its internal tfifo. When netem is used with a child qdisc, the child qdisc can use 'qdisc_tree_reduce_backlog' to inform its parent, netem, about created or dropped SKBs. This function updates 'qlen' and the backlog statistics of netem, but netem does not account for changes made by a child qdisc. 'qlen' then indicates the wrong number of packets in the tfifo. If a child qdisc creates new SKBs during enqueue and informs its parent about this, netem's 'qlen'	https://git.kern el.org/stable/c/ 10df49cfca73df bbdb6c4150d85 9f7e8926ae427, https://git.kern el.org/stable/c/ 216509dda290f 6db92c816dd54 b83c1df9da9e7 6, https://git.kern el.org/stable/c/ 356078a5c55ec 8d2061fcc009fb 8599f5b0527f9	O-LIN-LINU- 200125/1023

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			value is increased. When netem dequeues the newly created SKBs from the child, the 'qlen' in netem is not updated. If 'qlen' reaches the configured sch->limit, the enqueue function stops working, even though the tfifo is not full.		
			Reproduce the bug: Ensure that the sender machine has GSO enabled. Configure netem as root qdisc and tbf as its child on the outgoing interface of the machine as follows: \$ tc qdisc add dev <oif> root handle 1: netem delay 100ms limit 100 \$ tc qdisc add dev <oif> parent 1:0 tbf rate 50Mbit burst 1542 latency 50ms</oif></oif>		
			Send bulk TCP traffic out via this interface, e.g., by running an iPerf3 client on the machine. Check the qdisc statistics: \$ tc -s qdisc show dev <oif></oif>		
			Statistics after 10s of iPerf3 TCP test before the fix (note that netem's backlog > limit, netem stopped accepting packets): qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 2767766 bytes 1848 pkt (dropped 652, overlimits 0 requeues 0) backlog 4294528236b 1155p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 2767766 bytes 1848		
			pkt (dropped 327, overlimits 7601 requeues		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0)		
			backlog 0b 0p requeues 0		
			backing ob op requeues o		
			Statistics after the fix:		
			qdisc netem 1: root refcnt 2		
			limit 1000 delay 100ms		
			Sent 37766372 bytes		
			24974 pkt (dropped 9,		
			overlimits 0 requeues 0) backlog 0b 0p requeues 0		
			qdisc tbf 10: parent 1:1 rate		
			50Mbit burst 1537b lat		
			50ms		
			Sent 37766372 bytes		
			24974 pkt (dropped 327,		
			overlimits 96017 requeues		
			0)		
			backlog 0b 0p requeues 0		
			tbf segments the GSO SKBs		
			(tbf_segment) and updates		
			the netem's 'qlen'.		
			The interface fully stops		
			transferring packets and		
			"locks". In this case,		
			the child qdisc and tfifo are		
			empty, but 'qlen' indicates		
			the tfifo is at its limit and no more		
			packets are accepted.		
			packets are accepted.		
			This patch adds a counter		
			for the entries in the tfifo.		
			Netem's 'qlen' is		
			only decreased when a		
			packet is returned by its		
			dequeue function, and not during enqueuing into the		
			child qdisc. External		
			updates to 'qlen' are thus		
			accounted for and only the		
			behavior of the backlog		
			statistics changes. As		
			in other qdiscs, 'qlen' then		
			keeps track of how many		
			packets are held in netem and all of its children.		
			As before, sch->limit		
			remains as the		
			maximum number of		
			packets in the tfifo. The		
			same applies to netem's		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			backlog statistics.						
			CVE ID: CVE-2024-56770						
Affected Ver	Affected Version(s): From (including) 6.7 Up to (excluding) 6.12.8								
Use After Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries/vas: Add close() callback in vas_vm_ops struct The mapping VMA address is saved in VAS window struct when the paste address is mapped. This VMA address is used during migration to unmap the paste address if the window is active. The paste address mapping will be removed when the window is closed or with the munmap(). But the VMA address in the VAS window is not updated with munmap() which is causing invalid access during migration. The KASAN report shows: [16386.254991] BUG: KASAN: slab-use-after-free in reconfig_close_windows+0x 1a0/0x4e8 [16386.255043] Read of size 8 at addr c00000014a819670 by task drmgr/696928 [16386.255096] CPU: 29 UID: 0 PID: 696928 Comm: drmgr Kdump: loaded Tainted: G B 6.11.0-rc5-nxgzip #2 [16386.255128] Tainted: [B]=BAD_PAGE [16386.255148] Hardware name: IBM,9080-HEX	https://git.kern el.org/stable/c/ 05aa156e156ef 3168e7ab8a687 21945196495c1 7, https://git.kern el.org/stable/c/ 6d9cd27105459 f169993a4c5f21 6499a946dbf34, https://git.kern el.org/stable/c/ 8b2282b508452 1254a2cd9742a 3f4e1d5b77f843	O-LIN-LINU- 200125/1024				

0-1

4-5

5-6

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Power11 (architected) 0x820200 0xf000007 of:IBM,FW1110.00 (NH1110_016) hv:phyp pSeries [16386.255181] Call Trace: [16386.255202] [c00000016b297660] [c000000018ad0ac] dump_stack_lvl+0x84/0xe8 (unreliable) [16386.255246] [c00000016b297690] [c000000006e8a90] print_report+0x19c/0x764 [16386.255285] [c00000016b297760] [c000000006e9490] kasan_report+0x128/0x1f8 [16386.255309] [c00000016b297880] [c00000016b297880] [c00000016b297880] [c00000016b29780] [c00000016b2978a0] [c00000016b2978a0] [c00000016b297990] [c0000000013f898] reconfig_close_windows+0x 1a0/0x4e8 [16386.255343] [c00000016b297990] [c00000000140e58] vas_migration_handler+0x3 a4/0x3fc [16386.255368] [c00000016b297a90] [c000000000128848] pseries_migrate_partition+0 x4c/0x4c4		
			[16386.256136] Allocated by task 696554 on cpu 31 at 16377.277618s: [16386.256149] kasan_save_stack+0x34/0x 68 [16386.256163] kasan_save_track+0x34/0x 80 [16386.256175] kasan_save_alloc_info+0x58 /0x74		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_softirq_own_stack+0x6c /0x88 [16386.256509] do_softirq_own_stack+0x58 /0x88 [16386.256521]irq_exit_rcu+0x1a4/0x20c [16386.256533] irq_exit+0x20/0x38 [16386.256544] interrupt_async_exit_prepar e.constprop.0+0x18/0x2c		
			[16386.256717] Last potentially related work creation: [16386.256729] kasan_save_stack+0x34/0x 68 [16386.256741]kasan_record_aux_stack+0 xcc/0x12c [16386.256753]call_rcu_common.constpro p.0+0x94/0xd04 [16386.256766] vm_area_free+0x28/0x3c [16386.256778] remove_vma+0xf4/0x114 [16386.256797] do_vmi_align_munmap.cons tprop.0+0x684/0x870 [16386.256811]vm_munmap+0xe0/0x1f8 [16386.256821]		
			sys_munmap+0x54/0x6c [16386.256830] system_call_exception+0x1a 0/0x4a0 [16386.256841] system_call_vectored_comm on+0x15c/0x2ec [16386.256868] The buggy address belongs to the object at c00000014a819670 which belongs to the cache vm_area_struct of size 168		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address is located 0 bytes inside of freed 168-byte region [c00000014a819718]		
			[16386.256915] The buggy address belongs to the physical page: [16386.256928] page: refcount:1 mapcount:0 mapping:000000000000000000000000000000000000		
			CVE ID: CVE-2024-56765		
Use After Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ublk: detach gendisk from ublk device if add_disk() fails Inside ublk_abort_requests(), gendisk is grabbed for aborting all inflight requests. And ublk_abort_requests() is called when exiting the uring context or handling timeout. If add_disk() fails, the gendisk may have been freed when calling ublk_abort_requests(), so use-after-free can be caused when getting disk's reference in ublk_abort_requests().	https://git.kern el.org/stable/c/ 75cd4005da549 2129917a4a4ee 45e8166055610 4, https://git.kern el.org/stable/c/ 7d680f2f76a341 7fdfc3946da747 1e81464f7b41	O-LIN-LINU- 200125/1025

CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fixes the bug by detaching gendisk from ublk device if add_disk() fails. CVE ID: CVE-2024-56764		
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: PCI/MSI: Handle lack of irqdomain gracefully Alexandre observed a warning emitted from pci_msi_setup_msi_irqs() on a RISCV platform which does not provide PCI/MSI support: WARNING: CPU: 1 PID: 1 at drivers/pci/msi/msi.h:121 pci_msi_setup_msi_irqs+0x2 c/0x32 pci_enable_msix_range+0x 30c/0x596 pci_msi_setup_msi_irqs+0x2 c/0x32 pci_alloc_irq_vectors_affinit y+0xb8/0xe2 RISCV uses hierarchical interrupt domains and correctly does not implement the legacy fallback. The warning triggers from the legacy fallback stub. That warning is bogus as the PCI/MSI layer knows whether a PCI/MSI parent domain is associated with the device or not. There is a check for MSI-X, which has a legacy assumption. But that legacy	https://git.kern el.org/stable/c/ a60b990798eb1 7433d02837882 80422b1bd94b1 8, https://git.kern el.org/stable/c/ aed157301c659 a48f5564cc456 8cf0e5c8831af0, https://git.kern el.org/stable/c/ b1f7476e07b93 d65a1a3643dcb 4a7bed80d4328 d	O-LIN-LINU- 200125/1026

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fallback assumption is only valid when legacy support is enabled, but otherwise the check should simply return -ENOTSUPP.		
			Loongarch tripped over the same problem and blindly enabled legacy support without implementing the legacy fallbacks. There are weak implementations which return an error, so the problem was papered over.		
			Correct pci_msi_domain_supports() to evaluate the legacy mode and add the missing supported check into the MSI enable path to complete it.		
			CVE ID: CVE-2024-56760		
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: tracing: Prevent bad count for tracing_cpumask_write If a large count is provided, it will trigger a warning in bitmap_parse_user. Also check zero for it. CVE ID: CVE-2024-56763	https://git.kern el.org/stable/c/ 03041e474a6a8 f1bfd4b96b164 bb3165c48fa1a 3, https://git.kern el.org/stable/c/ 1cca920af19df5 dd91254e5ff35e 68e911683706, https://git.kern el.org/stable/c/ 3d15f4c244955 8ffe83b4dba306 14ef1cd6937c3	O-LIN-LINU- 200125/1027
Use of Uninitialized Resource	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: dvb-frontends: dib3000mb: fix uninit-value in dib3000_write_reg Syzbot reports [1] an uninitialized value issue	https://git.kern el.org/stable/c/ 1d6de21f00293 d819b5ca6dbe7 5ff1f3b6392140, https://git.kern el.org/stable/c/ 2dd59fe0e19e1 ab95525997808 2b62e5751924c	O-LIN-LINU- 200125/1028

0-1

4-5

5-6

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	found by KMSAN in dib3000_read_reg(). Local u8 rb[2] is used in i2c_transfer() as a read buffer; in case that call fails, the buffer may end up with some undefined values. Since no elaborate error handling is expected in dib3000_write_reg(), simply zero out rb buffer to mitigate the problem. [1] Syzkaller report	Patch 7, https://git.kern el.org/stable/c/ 3876e3a1c31a5 8a352c6bf5d2a 90e3304445a63 7	NCIIPC ID
			dvb-usb: bulk message failed: -22 (6/0) ====================================		
			dib3000mb_attach+0x2d8/ 0x3c0 drivers/media/dvb- frontends/dib3000mb.c:75 8 dibusb_dib3000mb_fronten d_attach+0x155/0x2f0 drivers/media/usb/dvb- usb/dibusb-mb.c:31		
			dvb_usb_adapter_frontend_i nit+0xed/0x9a0 drivers/media/usb/dvb- usb/dvb-usb-dvb.c:290 dvb_usb_adapter_init drivers/media/usb/dvb- usb/dvb-usb-init.c:90 [inline] dvb_usb_init drivers/media/usb/dvb- usb/dvb-usb-init.c:186 [inline]		

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dvb_usb_device_init+0x25a 8/0x3760 drivers/media/usb/dvb- usb/dvb-usb-init.c:310 dibusb_probe+0x46/0x250 drivers/media/usb/dvb- usb/dibusb-mb.c:110 Local variable rb created at: dib3000_read_reg+0x86/0x 4e0 drivers/media/dvb- frontends/dib3000mb.c:54 dib3000mb_attach+0x123/ 0x3c0 drivers/media/dvb- frontends/dib3000mb.c:75 8		
NULL Pointer Dereference	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: dmaengine: at_xdmac: avoid null_prt_deref in at_xdmac_prep_dma_memse t The at_xdmac_memset_create_d esc may return NULL, which will lead to a null pointer dereference. For example, the len input is error, or the atchan->free_descs_list is empty and memory is exhausted. Therefore, add check to avoid this. CVE ID: CVE-2024-56767	https://git.kern el.org/stable/c/ 54376d8d2659 6f98ed7432a78 8314bb9154bf3 e3, https://git.kern el.org/stable/c/ c43ec96e8d343 99bd9dab2f2dc 316b904892133 f, https://git.kern el.org/stable/c/ e658f1c133b85 4b2ae79914730 1d82dddb8f316 2	O-LIN-LINU- 200125/1029
Affected Vers	s <mark>ion(s): From (inc</mark>	cluding) 6	8 Up to (excluding) 6.12.4		
NULL Pointer Dereference	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: kunit: Fix potential null dereference in kunit_device_driver_test()	https://git.kern el.org/stable/c/ 435c20eed572a 95709b1536ff7 8832836b2f91b 1, https://git.kern	O-LIN-LINU- 200125/1030

CVSSv3 Scoring Scale
* stands for all versions

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kunit_kzalloc() may return a NULL pointer, dereferencing it without NULL check may lead to NULL dereference. Add a NULL check for test_state.	el.org/stable/c/ 5d28fac59369b 5d3c48cdf09e5 0275a61ff91202	
			CVE ID: CVE-2024-56773		
Vendor: Mic	rosoft				
Product: wii	ndows_10_21h2				
Affected Vers	sion(s): * Up to (e	xcluding)	10.0.19044.5371		
Heap-based Buffer Overflow	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21333	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21333	O-MIC-WIND- 200125/1031
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21334	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21334	O-MIC-WIND- 200125/1032
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21335	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21335	O-MIC-WIND- 200125/1033
Product: wii	ndows_10_22h2				
Affected Vers	sion(s): * Up to (e	xcluding)	10.0.19045.5371		
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21335	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21335	O-MIC-WIND- 200125/1034
Heap-based Buffer Overflow	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21333	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21333	O-MIC-WIND- 200125/1035
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege	https://msrc.mi crosoft.com/upd ate-	O-MIC-WIND- 200125/1036

CVSSv3 Scoring Scale
* stands for all versions

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability CVE ID: CVE-2025-21334	guide/vulnerabi lity/CVE-2025- 21334	
Product: wii	ndows_11_22h2			21331	
Affected Vers	sion(s): * Up to (e	xcluding)	10.0.22621.4751		
Heap-based Buffer Overflow	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21333	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21333	O-MIC-WIND- 200125/1037
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21334	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21334	O-MIC-WIND- 200125/1038
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21335	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21335	O-MIC-WIND- 200125/1039
Product: wii	ndows_11_23h2				
Affected Vers	sion(s): * Up to (e	xcluding)	10.0.22621.4751		
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21335	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21335	O-MIC-WIND- 200125/1040
Heap-based Buffer Overflow	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21333	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21333	O-MIC-WIND- 200125/1041
Affected Vers	sion(s): * Up to (e	xcluding)	10.0.22631.4751		
Heap-based Buffer Overflow	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21333	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21333	O-MIC-WIND- 200125/1042
Use After	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege	https://msrc.mi crosoft.com/upd ate-	O-MIC-WIND- 200125/1043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21334	lity/CVE-2025- 21334	
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21335	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21335	O-MIC-WIND- 200125/1044
Product: win	ndows_11_24h2				
Affected Vers	sion(s): * Up to (e	excluding)	10.0.26100.2894		
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21335	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21335	O-MIC-WIND- 200125/1045
Heap-based Buffer Overflow	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21333	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21333	O-MIC-WIND- 200125/1046
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21334	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21334	O-MIC-WIND- 200125/1047
Product: wii	ndows_server_2	022_23h2			
Affected Vers	sion(s): * Up to (e	excluding)	10.0.25398.1369		
Heap-based Buffer Overflow	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21333	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21333	O-MIC-WIND- 200125/1048
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21334	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21334	O-MIC-WIND- 200125/1049
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21335	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21335	O-MIC-WIND- 200125/1050

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wir	ndows_server_2	025	1		
			10.0.26100.2894		
Threeted vers		keruumgj	Windows Hyper-V NT	https://mara.mi	
Use After Free	14-Jan-2025	7.8	Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21334	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21334	O-MIC-WIND- 200125/1051
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21335	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21335	O-MIC-WIND- 200125/1052
Heap-based Buffer Overflow	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability CVE ID: CVE-2025-21333	https://msrc.mi crosoft.com/upd ate- guide/vulnerabi lity/CVE-2025- 21333	O-MIC-WIND- 200125/1053
Vendor: Qua	lcomm				
Product: agt	:1000_firmware				
Affected Vers					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-AQT1- 200125/1054
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-AQT1- 200125/1055
Product: ar8	3035_firmware				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-AR80- 200125/1056

0-1

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arise.		
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-AR80- 200125/1057
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-AR80- 200125/1058
Due desets a se	2 0150 G		CVE ID: CVE-2024-33007	bunetiii.iitiiii	
	2x_9150_firmwa	are			
Affected Vers	sion(s): -				l
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-C-V2- 200125/1059
Product: cer	8811_firmware		CVE 1D. CVE 2021 33007	bancanina	
Affected Vers					
Affected vers	sion(s): -		The post of DOC		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-CSR8- 200125/1060
Product: cer	b31024_firmw a	re			
Affected Vers					
Allected vers	1011(8)		Information disclosure	https://docs.qu	
Buffer Over- read	06-Jan-2025	6.1	while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-CSRB- 200125/1061

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33067	bulletin.html	
Product: fas	tconnect_6200_	firmware			
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-FAST- 200125/1062
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-FAST- 200125/1063
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-FAST- 200125/1064
Product: fas	tconnect_6700_	firmware			
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-FAST- 200125/1065
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-FAST- 200125/1066
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is	https://docs.qu alcomm.com/pr oduct/publicres ources/security	0-QUA-FAST- 200125/1067

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removed from the global list while another thread is using it for a process- specific task, issues may arise.	bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45553		
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-FAST- 200125/1068
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-FAST- 200125/1069
Product: fast	tconnect_6800_t	firmware		builetii.iitiiii	
Affected Vers					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-FAST- 200125/1070
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-FAST- 200125/1071
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-FAST- 200125/1072
Product: fas	tconnect_6900_	firmware			
	. ()				
Affected Vers	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1073
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-FAST- 200125/1074
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-FAST- 200125/1075
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-FAST- 200125/1076
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-FAST- 200125/1077
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. CVE ID: CVE-2024-45548	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-FAST- 200125/1078
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-FAST- 200125/1079

3-4

2-3

4-5

5-6

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45550	bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-FAST- 200125/1080
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-FAST- 200125/1081
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-FAST- 200125/1082
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-FAST- 200125/1083
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-FAST- 200125/1084
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-FAST- 200125/1085
Product: fastconnect_7800_firmware					
Affected Version(s): -					
Buffer Copy 06-Jan-2025 8.4 Memory corruption while https://docs.qu 0-QUA-FAST-					
CVSSv3 Scoring	Scale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1086
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. CVE ID: CVE-2024-45548	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-FAST- 200125/1087
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-FAST- 200125/1088
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-FAST- 200125/1089
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. CVE ID: CVE-2024-45550	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-FAST- 200125/1090
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-FAST- 200125/1091
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	0-QUA-FAST- 200125/1092

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID: CVE-2024-45542	-2025- bulletin.html		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-FAST- 200125/1093	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-FAST- 200125/1094	
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-FAST- 200125/1095	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-FAST- 200125/1096	
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-FAST- 200125/1097	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-FAST- 200125/1098	
Product: flig	ht_rb5_5g_firmv	ware		1		
Affected Vers	ion(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific	https://docs.qu alcomm.com/pr	0-QUA-FLIG- 200125/1099	
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45553		
Product: imi	mersive_home_2	214_firmv	vare		
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-IMME- 200125/1100
			CVE ID: CVE-2024-45558	bulletin.html	
Product: imi	mersive_home_2	216_firmv	vare		
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-IMME- 200125/1101
			CVE ID: CVE-2024-45558	bulletin.html	
Product: imi	mersive_home_3	316_firmv	vare		
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-IMME- 200125/1102
D d :		10 G		bulletin.html	
Affected Vers	mersive_home_3	18_IIFMV	vare		
Aniecteu vers	ion(s)		Transient DOS can occur	https://docs.gv	
Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	O-QUA-IMME- 200125/1103

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			length. CVE ID: CVE-2024-45558	-2025- bulletin.html		
Product: im	nersive_home_3	3210_firm	iware			
Affected Vers	ion(s): -					
Buffer Over- read 06-Jan-2025		7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-IMME- 200125/1104	
Product: imi	nersive_home_3	326_firmv	vare			
Affected Vers	ion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-IMME- 200125/1105	
Product: ipq	5010_firmware					
Affected Vers	ion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-IPQ5- 200125/1106	
			CVE ID: CVE-2024-45558	bulletin.html		
Product: ipq	5028_firmware					
Affected Vers	ion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-IPQ5- 200125/1107	
			CVE ID: CVE-2024-45558	bulletin.html		
Product: ipq	5300_firmware					
	ion(s): -					

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVF ID	Patch	NCIIPC ID
weakness	Publish Date	CVSSVS	Description & CVE ID	Paten	NCIIPCID
Buffer Over- read	1 06-1an-2025		Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-IPQ5- 200125/1108
Product: ipq	5302_firmware				
Affected Vers	sion(s): -				
Buffer Over-read 06-Jan-2025		7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-IPQ5- 200125/1109
Product: ipq	5312_firmware				
Affected Vers					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-IPQ5- 200125/1110
			CVE ID: CVE-2024-45558	bulletin.html	
Product: ipq	5332_firmware				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-IPQ5- 200125/1111
Product: ipa	6000_firmware				
Affected Vers					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-IPQ6- 200125/1112

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID: CVE-2024-45558	bulletin.html		
Product: ipq	6010_firmware					
Affected Vers	sion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-IPQ6- 200125/1113	
Product: ipq	6018_firmware					
Affected Vers	sion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-IPQ6- 200125/1114	
			CVE ID: CVE-2024-45558	bulletin.html		
Product: ipq	6028_firmware					
Affected Vers	sion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-IPQ6- 200125/1115	
			CVE ID: CVE-2024-45558	bulletin.html		
Product: ipq	8070a_firmwar	e				
Affected Vers	sion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-IPQ8- 200125/1116	
			CVE ID: CVE-2024-45558	bulletin.html		
Product: ipq	8071a_firmwar	e				
Affected Vers	sion(s): -					
	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	O-QUA-IPQ8-	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1117	
Product: ipq	8072a_firmwar	e			1	
Affected Vers	sion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-IPQ8- 200125/1118	
Product: inc	 8074a_firmwar	0	CVL ID. CVL 2024 43330	builetiii.iitiiii		
Affected Vers						
Threeted Vers			Transient DOS can occur			
Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-IPQ8- 200125/1119	
			CVE ID: CVE-2024-45558	bulletin.html		
Product: ipq	 8076a_firmwar	e				
Affected Vers	sion(s): -					
Buffer Over-read 06-Jan-2025 7.5		7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-IPQ8- 200125/1120	
Product: ipq	8076_firmware					
Affected Vers	sion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-IPQ8- 200125/1121	

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date CVSSv		Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558		
Product: ipq	8078a_firmwar	e			
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-IPQ8- 200125/1122
Product: ipq	8078_firmware				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-IPQ8- 200125/1123
Product: ipq	8173_firmware				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-IPQ8- 200125/1124
			CVE ID: CVE-2024-45558	bulletin.html	
Product: ipq	8174_firmware				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-IPQ8- 200125/1125
Product: ipa	9008_firmware				
Affected Vers					
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	O-QUA-IPQ9-
	,			/ / 1	
CVSSv3 Scoring	Scale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Veakness Publish Date		Description & CVE ID	Patch	NCIIPC ID	
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1126	
Product: ipq	9048_firmware					
Affected Vers	sion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-IPQ9- 200125/1127	
Product: inc	 9554_firmware					
Affected Vers						
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-IPQ9- 200125/1128	
			CVE ID: CVE-2024-45558	bulletin.html		
Product: ipq	9570_firmware					
Affected Vers	sion(s): -					
Buffer Over-read 06-Jan-2025 7.5		7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-IPQ9- 200125/1129	
Product: ipq	 9574_firmware					
Affected Vers	sion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-IPQ9- 200125/1130	

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID: CVE-2024-45558			
Product: ms	m8996au_firmv	vare				
Affected Vers	ion(s): -					
Buffer Over-		ds 06-Jan-2025 8.4 programs to b		https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-MSM8- 200125/1131	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-MSM8- 200125/1132	
Product: qar	n8255p_firmwa	re				
Affected Vers						
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1133	
			CVE ID: CVE-2024-45555			
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QAM8- 200125/1134	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
N/A	06-Jan-2025 7.5		Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU.		0-QUA-QAM8- 200125/1135	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	-2025- bulletin.html https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QAM8- 200125/1136	
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QAM8- 200125/1137	
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1138	
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1139	
Product: qai	m8295p_firmwa	ire			l	
Affected Vers	sion(s): -					
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1140	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				_	_		_	_		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1141
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 https://docs alcomm.com oduct/public ources/secur bulletin/janu-2025-bulletin.html		O-QUA-QAM8- 200125/1142
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1143
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1144
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1145
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QAM8- 200125/1146
Buffer Over-	06-Jan-2025	6.1	Information disclosure	https://docs.qu	O-QUA-QAM8-

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1147
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1148
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1149
Product: qai	n8620p_firmwa	re			
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1150
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1151
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the	https://docs.qu alcomm.com/pr oduct/publicres ources/security	0-QUA-QAM8- 200125/1152

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global registers through SMMU. CVE ID: CVE-2024-43064	bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1153
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1154
Product: qai	m8650p_firmwa	ire			
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1155
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QAM8- 200125/1156
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-QAM8- 200125/1157

4-5

5-6

6-7

3-4

2-3

8-9

9-10

06-Jan-2025		CVE ID: CVE-2024-45558	bulletin.html	
06-Jan-2025		H		
00 juli 2023	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1158
06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1159
06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1160
06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-QAM8- 200125/1161
18775p_firmwa	re		builetiii.iitiiii	
on(s): -				
06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1162
		CVE ID: CVE-2024-45555		
06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	O-QUA-QAM8- 200125/1163
	06-Jan-2025 8775p_firmwa on(s): -	06-Jan-2025 6.1 8775p_firmware on(s): - 06-Jan-2025 8.4	CVE ID: CVE-2024-43064 Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366 information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063 Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559 8775p_firmware On(s): Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555 Memory corruption can occur when process-specific maps are added to the global list. If a map is	CVE ID: CVE-2024-43064 bulletin.html Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366 bulletin.html CVE ID: CVE-2024-23366 bulletin.january -2025-bulletin.html Information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063 CVE ID: CVE-2024-43063 Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559 CVE ID: CVE-2024-45559 R775p_firmware On(s):- Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555 Memory corruption can occur when process-specific atampered IFS2 system image. CVE ID: CVE-2024-45555 Memory corruption can occur when process-specific atampered IFS2 system image. CVE ID: CVE-2024-45555 Memory corruption can occur when process-specific atampered IFS2 system image. CVE ID: CVE-2024-45555 Memory corruption can occur when process-specific atampered IFS2 system image. CVE ID: CVE-2024-45555 Memory corruption can occur when process-specific atampered IFS2 system image. CVE ID: CVE-2024-45555 Memory corruption can occur when process-specific atampered icomm.com/product/publicres ources/security bulletin.html

5-6

6-7

7-8

9-10

3-4

Publish Date	CVSSv3	Description & CVE ID Patch		NCIIPC ID
		while another thread is using it for a process-specific task, issues may arise.	-2025- bulletin.html	
		CVE ID: CVE-2024-45553		
06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1164
06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QAM8- 200125/1165
06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1166
06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1167
06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAM8- 200125/1168
nsrv1h_firmwai	re			
ion(s): -				
06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	0-QUA-QAMS- 200125/1169
	06-Jan-2025 06-Jan-2025 06-Jan-2025 06-Jan-2025 msrv1h_firmwarsion(s): -	06-Jan-2025 7.5 06-Jan-2025 6.6 06-Jan-2025 5.5 msrv1h_firmware sion(s): -	while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366 information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063 Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559 msrv1h_firmware sion(s):- Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification.	while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366 O6-Jan-2025 6.1 ransient DOS can occur while invoking the mailbox read API. CVE ID: CVE-2024-23366 Uncontrolled resource devices the product/publicres ources/security bulletin/january -2025- bulletin.html https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	kness Publish Date CVSSv3 Description & CVE ID			Patch	NCIIPC ID
			programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	-2025- bulletin.html	
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAMS- 200125/1170
			CVE ID: CVE-2024-45553		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAMS- 200125/1171
			Transient DOS can occur	bulletin.html	
Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-QAMS- 200125/1172
			CVE ID: CVE-2024-45558	bulletin.html	
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAMS- 200125/1173
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAMS- 200125/1174
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-	https://docs.qu alcomm.com/pr oduct/publicres	0-QUA-QAMS- 200125/1175

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			FastRPC backend. CVE ID: CVE-2024-45559	ources/security bulletin/january -2025- bulletin.html		
-	nsrv1m_firmwa	re				
Affected Vers	ion(s): -					
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAMS- 200125/1176	
			CVE ID: CVE-2024-45555			
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QAMS- 200125/1177	
			CVE ID: CVE-2024-45553			
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QAMS- 200125/1178	
			Transient DOS can occur			
Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QAMS- 200125/1179	
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	0-QUA-QAMS- 200125/1180	

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45559	-2025- bulletin.html	
Product: qca	0000_firmware				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA0- 200125/1181
Product: aca	1062_firmware				
Affected Vers		•			
	ion(s)			httms://da.a.a	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA1- 200125/1182
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA1- 200125/1183
Product: qca	1064_firmware			banetiiiitiiii	
Affected Vers	ion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA1- 200125/1184
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA1- 200125/1185
Product: qca	2062_firmware				
Affected Vers	ion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA2- 200125/1186
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA2- 200125/1187
Product: qca	2064_firmware				
Affected Vers	ion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA2- 200125/1188
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA2- 200125/1189
	2065_firmware				
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA2- 200125/1190
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA2- 200125/1191
Product: qca	2066_firmware				
	ion(s): -				

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Woolmass	Dublish Data	CVCC2	Description & CVE ID	Datah	NCHDC ID
Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA2- 200125/1192
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA2- 200125/1193
Product: qca	4024_firmware				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA4- 200125/1194
			CVE ID: CVE-2024-45558	buneun.numi	
	16174a_firmwar	e			
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1195
			CVE ID: CVE-2024-45553		
Product: qca	16310_firmware	!			
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1196

read 06-Jan-2025 S.1 valid opcode received from sound model driver. CVE ID: CVE-2024-33067 bulletin.january 2025-bulletin.html 200125/11st 20012	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over- read O6-Jan-2025 6.1 Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067 Product: qca6391_firmware Affected Version(s):- Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Buffer Copy without Checking Size of Input (*Classic Buffer Overflow*) Stack-based Buffer Overflow O6-Jan-2025 A8 Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541 Wemory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541 Wemory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541 Wemory corruption when IOCTL call is invoked from user-space to write board data. CVE ID: CVE-2024-45542 Wemory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542 Use After O6-Jan-2025 Buffer Copy without Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542 Delletin,html Information disclosure while invoking callback function of sound model driver while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver from ADSP for every valid opcode received from sound model driver may be used to the global list. If a map is a cource/security bulletin/january -2025- bulletin.html Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver from ADSP for every valid opcode received from sound model driver from ADSP for every valid opcode received from sound model driver from ADSP for every valid opcode received from sound model driver from	Product: qca	16320_firmware	:			
Buffer Over- read 06-Jan-2025 6.1 while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067 Wemory corruption can occur when process-specific maps are added to the global list. If a map is removed from using it for a process-specific maps are added to the global list. If a map is removed from using it for a process-specific maps are added to the global list. If a map is removed from using it for a process-specific map is removed from using it for a process-specific map is removed from using it for a process-specific map is removed from the global list. If a map is removed from the global list. If a map is removed from the global list. If a map is removed from the global list. If a map is removed from the global list. If a map	Affected Vers	sion(s): -				
Affected Version(s): - Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553		06-Jan-2025	6.1	while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCA6- 200125/1197
Wemory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	Product: qca	6391_firmware				
Use After Free O6-Jan-2025 7.8 Buffer Copy without (Classic Buffer Overflow) Stack-based Buffer Overflow Buffer Overflow O6-Jan-2025 7.8 Buffer Overread O6-Jan-2025 7.8 Buffer Overflow O6-Jan-2025 7.8 O6-Jan-2025 7	Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') Table 19		06-Jan-2025	7.8	occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCA6- 200125/1198
Stack-based Buffer Overflow 7.8 Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542 Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver O-QUA-QCA 200125/120 0-QUA-QCA 200125/120 0-QUA-QCA 200125/120 0-QUA-QCA 200125/120 0-QUA-QCA 200125/120 0-QUA-QCA 200125/120	without Checking Size of Input ('Classic Buffer	06-Jan-2025	7.8	IOCTL call is invoked from user-space to read board data.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCA6- 200125/1199
Buffer Overread O6-Jan-2025 while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. while invoking callback function of sound model driver oduct/publicres ources/security bulletin/january	Stack-based Buffer	06-Jan-2025	7.8	IOCTL call is invoked from user-space to write board data to WLAN driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-QCA6- 200125/1200
CVE ID: CVE-2024-33067 bulletin.html		06-Jan-2025	6.1	while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-QCA6- 200125/1201
Product: qca6420_firmware	Product: qca	16420_firmware	:			
Affected Version(s): -						

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
	- 40-10-1-2 4:00	213313	Memory corruption when	https://docs.qu alcomm.com/pr	110111 0 12
Stack-based Buffer	06-Jan-2025	7.8	IOCTL call is invoked from user-space to write board data to WLAN driver.	oduct/publicres ources/security	O-QUA-QCA6- 200125/1202
Overflow			CVE ID: CVE-2024-45542	bulletin/january -2025- bulletin.html	200123/1202
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1203
Product: qca	6426_firmware				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCA6- 200125/1204
			CVE ID: CVE-2024-33067	bulletin.html	
Product: qca	6430_firmware				
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	O-QUA-QCA6- 200125/1205
Buffer Overflow')			CVE ID: CVE-2024-45541	-2025- bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1206
Product: gca	6436_firmware			bunean.nam	
Affected Vers					
	(0).		Information disclosure	https://docs.qu	
Buffer Over- read	06-Jan-2025	6.1	while invoking callback function of sound model driver from ADSP for every valid opcode received from	alcomm.com/pr oduct/publicres ources/security bulletin/january	O-QUA-QCA6- 200125/1207

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33067	bulletin.html	
Product: qca	16554a_firmwar	·e			
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA6- 200125/1208
D 1 .			CVE ID: CVE-2024-45550	bulletin.html	
	16564au_firmwa	are			
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1209
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA6- 200125/1210
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA6- 200125/1211
Product: qca	16564a_firmwar	e			
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten,	https://docs.qu alcomm.com/pr oduct/publicres	O-QUA-QCA6- 200125/1212

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	ources/security bulletin/january -2025- bulletin.html	
		CVE ID: CVE-2024-45555		
06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-QCA6- 200125/1213
		CVE ID: CVE-2024-33067	bulletin.html	
16574au_firmwa	ire			
sion(s): -				
06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1214
		CVE ID: CVE-2024-45555		
06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1215
		CVE ID: CVE-2024-45553		
06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1216
	06-Jan-2025 06-Jan-2025 06-Jan-2025	06-Jan-2025 6.1 06-Jan-2025 8.4 06-Jan-2025 7.8	bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555 Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067 Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555 Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555 Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067 Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555 Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element to access the EXTN element to without checking the IE length

CVSSv3 Scoring Scale
* stands for all versions

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1217
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1218
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1219
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1220
Product: aca	16574a_firmwar	· · ·	CVL 1D. CVL 202+ 33007	Builetiii.iitiiii	
Affected Vers		. C			
Affected vers	31011(8)		Memory corruption can		
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1221
			Memory corruption can	https://docs.qu	
Use After Free	06-Jan-2025	7.8	occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCA6- 200125/1222

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using it for a process- specific task, issues may arise.	bulletin.html	
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1223
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCA6- 200125/1224
			CVE ID: CVE-2024-33067	bulletin.html	
Product: qca	a6574_firmware				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1225
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCA6- 200125/1226
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qca	a6584au_firmwa	are			
1 66 1 7 7	sion(s): -				
Affected Vers			Memory corruption can	https://docs.qu	

4-5

5-6

3-4

2-3

8-9

9-10

This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFSZ system image. CVE ID: CVE-2024-45555 Buffer Overread O6-Jan-2025 Buffer Overread O6-Jan-2025 Tansient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Buffer Overread O6-Jan-2025 To Standard Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Use After Off-Jan-2025 Differmation disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067 Product: qca6595au_firmware Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing box terification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a lampered IFS2 system image. CVE ID: CVE-2024-45555 Write Write This allows unauthorized product/publicres ources/security bulletin/January 2025-bulletin.html	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list. If a map is removed the per STA profile IE and tries in this profile IE and tries in th				programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system	-2025-	
Use After Free O6-Jan-2025 7.8				CVE ID: CVE-2024-45555		
Buffer Over-read 06-Jan-2025 7.5 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 CVE ID: CVE-2024-45558 Dilletin. CVE ID: CVE-2024-45558 CVE ID: CVE-2024-45555 CVE ID:		06-Jan-2025	7.8	occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process- specific task, issues may	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	
Buffer Over-read 06-Jan-2025 7.5 06-Jan-2025 7.5 06-Jan-2025 7.5 06-Jan-2025 06-Jan-2025 8.4 when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 CVE ID: CVE-2024-45558 Dilletin.html https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin.html https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin.html https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin.html Product: qca6595au_firmware Affected Version(s):- Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555 Dilletin.html				CVE ID: CVE-2024-45553		
Buffer Over- read 06-Jan-2025 6.1 while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067 bulletin.html 0-QUA-QCA6-200125/1230 Product: qca6595au_firmware Affected Version(s): - Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555 bulletin.html 0-QUA-QCA6-200125/1231 CVE ID: CVE-2024-45555		06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	
Product: qca6595au_firmware Affected Version(s): - Out-of-bounds Write O6-Jan-2025 8.4 Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555 CVE ID: CVE-2024-45555		06-Jan-2025	6.1	while invoking callback function of sound model driver from ADSP for every valid opcode received from	alcomm.com/pr oduct/publicres ources/security bulletin/january	
Affected Version(s): - Out-of-bounds Write O6-Jan-2025				CVE ID: CVE-2024-33067	bulletin.html	
Out-of-bounds Write Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555 Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	-		are			
Out-of-bounds Write 06-Jan-2025 8.4 06-Jan-2025 8.4 06-Jan-2025 8.4 Out-of-bounds Write 06-Jan-2025 8.4 Occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555 CVE ID: CVE-2024-45555	Affected Vers	ion(s): -				I
	bounds	06-Jan-2025	8.4	occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	
	Use After	06-Jan-2025	7.8	Memory corruption can	https://docs.qu	O-QUA-QCA6-

CVSSv3 Scoring Scale
* stands for all versions

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Free			occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1232
				https://docs.qu	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1233
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1234
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1235
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1236
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1237
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every	https://docs.qu alcomm.com/pr oduct/publicres ources/security	0-QUA-QCA6- 200125/1238

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			valid opcode received from sound model driver. CVE ID: CVE-2024-33067	bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA6- 200125/1239
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	O-QUA-QCA6- 200125/1240
			CVE ID: CVE-2024-45559	-2025- bulletin.html	
Product: qca	6595_firmware				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1241
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1242
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1243

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43064		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1244
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1245
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA6- 200125/1246
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA6- 200125/1247
Product: qca	16678aq_firmwa	ire			
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1248
Product: qca	16688aq_firmwa	ire			
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCA6- 200125/1249

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security-sensitive images, enabling the booting of a tampered IFS2 system image.	bulletin.html	
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1250
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCA6- 200125/1251
			CVE ID: CVE-2024-45558	bulletin.html	
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCA6- 200125/1252
			CVE ID: CVE-2024-43064	bulletin.html	
Product: qca	16696_firmware	;			
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1253
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the	https://docs.qu alcomm.com/pr oduct/publicres	0-QUA-QCA6- 200125/1254

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global list. If a map is removed from the global list while another thread is using it for a process- specific task, issues may arise.	ources/security bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45553		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-QCA6- 200125/1255
			CVE ID: CVE-2024-43064	bulletin.html	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-QCA6- 200125/1256
			CVE ID: CVE-2024-45558	bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA6- 200125/1257
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA6- 200125/1258
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-QCA6- 200125/1259
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCA6- 200125/1260

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA6- 200125/1261
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1262
Product: qca	16698aq_firmwa	are			
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1263
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA6- 200125/1264
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1265
			CVE ID: CVE-2024-45550	Duneum.num	

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1266	
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1267	
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1268	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1269	
Product: qca	16777aq_firmwa	ıre				
Affected Vers	sion(s): -					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1270	
Product: qca6787aq_firmware						
Affected Version(s): -						
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1271	

0-1

4-5

5-6

3-4

2-3

8-9

9-10

Product: qca6	6797ag firmwa				
•	6797ag firmwa		CVE ID: CVE-2024-45558		
Affected Versi	o, , , aq_m mwa	are			
1	on(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1272
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA6- 200125/1273
Product: qca8	8075_firmware				
Affected Versi	on(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA8- 200125/1274
Product: qca	8081_firmware	<u> </u>			
Affected Versi	on(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA8- 200125/1275
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	O-QUA-QCA8-

4-5

5-6

6-7

3-4

2-3

8-9

9-10

	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1276
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA8- 200125/1277
Product: qca	18082_firmware				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA8- 200125/1278
Product: qca	18084_firmware				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCA8- 200125/1279
.			CVE ID: CVE-2024-45558	bulletin.html	
	18085_firmware				
Affected Vers	sion(s): -				l
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA8- 200125/1280
Dun der et	18337_firmware				

CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9
--

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): -				
Use After Free 06-Jan-2025		7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCA8- 200125/1281
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA8- 200125/1282
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-QCA8- 200125/1283
			CVE ID: CVE-2024-33067	bulletin.html	
Product: qca	18386_firmware	:			
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCA8- 200125/1284
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qca	19367_firmware				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA9- 200125/1285

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca	19377_firmware				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067		https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA9- 200125/1286
Droduct, acc	19888_firmware		CVE1D: CVE 2021 33007	buile till.ittill	
-		,			
Affected Vers	sion(s): -		I m		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCA9- 200125/1287
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qca	19889_firmware				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCA9- 200125/1288
Droduct: acc	2073_firmware		CVL 1D. CVL 2024 43330	Builetiii.iitiiii	
Affected Vers	ion(s): -		M		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCC2- 200125/1289
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. CVE ID: CVE-2024-45548	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCC2- 200125/1290

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCC2- 200125/1291
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCC2- 200125/1292
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCC2- 200125/1293
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCC2- 200125/1294
_			CVE ID. CVE-2024-43330	bunetin.ntim	
	:2076_firmware	!			
Affected Vers	sion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCC2- 200125/1295
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCC2- 200125/1296
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call.	https://docs.qu alcomm.com/pr oduct/publicres ources/security	0-QUA-QCC2- 200125/1297

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45548	bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCC2- 200125/1298
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCC2- 200125/1299
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCC2- 200125/1300
Product: qcc	710_firmware				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCC7- 200125/1301
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCC7- 200125/1302
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model	https://docs.qu alcomm.com/pr oduct/publicres	O-QUA-QCC7- 200125/1303

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	ources/security bulletin/january -2025- bulletin.html	
Product: qcf	 8000sfp_firmwa	are			
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCF8- 200125/1304
Droduct: act	8000_firmware		CVL ID. CVL-2024-43330	Builetiii.iitiiii	
Affected Vers					
Affected vers			Transient DOS can occur		
Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-QCF8- 200125/1305
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qcf	8001_firmware				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCF8- 200125/1306
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qci	n4325_firmwar	e			
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCM4- 200125/1307

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date CVSSv3		Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45553		
Product: qcr	n4490_firmwar	e			
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCM4- 200125/1308
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCM4- 200125/1309
			CVE ID: CVE-2024-45553		
Product: qcn	n5430_firmwar	е			
Affected Vers	sion(s): -				
without Checking Size of Input ('Classic Buffer	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCM5- 200125/1310
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') Stack-based Buffer Overflow	06-Jan-2025 06-Jan-2025	7.8	IOCTL call is invoked from user-space to read board data.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	
without Checking Size of Input ('Classic Buffer Overflow') Stack-based Buffer			IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541 Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	200125/1310 O-QUA-QCM5-

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): -				
Stack-based Buffer Overflow	tack-based Buffer Obverflow Obverflow IOCTL causer-spa data to W		Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCM6- 200125/1313
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCM6- 200125/1314
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCM6- 200125/1315
Product: acr	n8550_firmwar	Α	CVE ID. CVE-2024-43330	bunetiii.iitiiii	
-					
Affected Version(s): - Buffer Over-read 06-Jan-2025		7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCM8- 200125/1316
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCM8- 200125/1317
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCM8- 200125/1318
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to	https://docs.qu alcomm.com/pr	O-QUA-QCM8- 200125/1319

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unmap the DMA buffers.	oduct/publicres ources/security	
			CVE ID: CVE-2024-33055	bulletin/january -2025-	
Droduati gar	5022 firmywana			bulletin.html	
Affected Vers	15022_firmware				
Allected vers	1011(8)		Transient DOS can occur		
Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCN5- 200125/1320
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qcr	15024_firmware	•			
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCN5- 200125/1321
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qcr	15052_firmware	•			
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCN5- 200125/1322
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qcr	15122_firmware)			
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCN5- 200125/1323
Product: acr	15124_firmware				
i roduct. qti	13147_III IIIWal t				

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCN5- 200125/1324
Product: qcn	15152_firmware	9			
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCN5- 200125/1325
D 1 .			CVE ID: CVE-2024-45558	bulletin.html	
-	15154_firmware				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCN5- 200125/1326
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qcn	15164_firmware	9			
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCN5- 200125/1327
Product: acr	16023_firmware	.			
Affected Vers					
Infected vers	1011(0).		Transient DOS can occur	https://docs.qu	
Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	alcomm.com/pr oduct/publicres ources/security bulletin/january	0-QUA-QCN6- 200125/1328

Product: qcn6112_firmware Affected Version(s): - Buffer Overread O6-Jan-2025 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. O-QUA 200125 O-QUA 200125 O-QUA 200125 O-QUA 200125 O-QUA 200126 O-QUA 200126 O-QUA 200126 O-QUA 200127 O-QUA 200127 O-QUA 200128 O-QUA 200128 O-QUA 200128 O-QUA 200129 O-QUA 200129	NCIIPC ID	Patch	Description & CVE ID	CVSSv3	Publish Date	Weakness
Affected Version(s): - Buffer Overread 06-Jan-2025 7.5 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. Transient DOS can occur when the driver parses the per STA profile IE and tries to access						
Buffer Over- read 06-Jan-2025 7.5 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 bulletin.html 0-QUA 20012: bulletin.h				:	16024_firmware	Product: qcr
when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the II length. CVE ID: CVE-2024-45558 Product: qcn6112_firmware Affected Version(s): Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the II length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the II length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the II length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the II length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the II length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the II length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the II length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the II length. CVE ID: CVE-2024-45558 Drive ID: CVE-2024-45558					ion(s): -	Affected Vers
Affected Version(s): - Buffer Over-read	UA-QCN6- 125/1329	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	7.5	06-Jan-2025	
Buffer Over- read 06-Jan-2025 7.5 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Product: qcn6122_firmware Affected Version(s): Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries ources/security bulletin/january -2025- bulletin.html Product: qcn6132_firmware Affected Version(s): - Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE per STA profile IE and tries to access the EXTN element per STA profile IE and tries to access the EXTN element ID without checking the IE per STA profile IE and tries to access the EXTN element ID without checking the IE per STA profile IE and tries to access the EXTN element ID without checking the IE per STA profile IE and tries to access the EXTN element ID without checking the IE per STA profile IE and tries to access the EXTN element ID without checking the IE per STA profile IE and tries to access the EXTN element ID without checking the IE per STA profile IE and tries to access the EXTN element ID without checking the IE					6112_firmware	Product: qcr
when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Product: qcn6122_firmware Affected Version(s): Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Do-QUA: 200125					ion(s): -	Affected Vers
Affected Version(s): - Buffer Overread O6-Jan-2025 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 CVE ID: CVE-2024-45558 CVE ID: CVE-2024-45558 CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. O-QUA-200125 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. O-QUA-200125 O-QUA-20012	UA-QCN6- 125/1330	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	7.5	06-Jan-2025	
Buffer Over- read O6-Jan-2025 7.5 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 CVE ID: CVE-2024-45558 CVE ID: CVE-2024-45558 CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE without checki					16122_firmware	Product: qcr
when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Product: qcn6132_firmware Affected Version(s): - Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE wildering diagnostry of the per STA profile IE and tries to access the EXTN element ID without checking the IE wildetin diagnostry allowed alcomm.com/product/publicres ources/security bulletin diagnostry alcomm.com/product/publicres/publicr					ion(s): -	Affected Vers
Product: qcn6132_firmware Affected Version(s): - Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE O6-Jan-2025 7.5 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ources/security bulletin/ianuary 200125	UA-QCN6- 125/1331	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	7.5	06-Jan-2025	
Affected Version(s): - Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE O6-Jan-2025 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ources/security bullotin/ianuary 200125		bulletin.html	CVE ID: CVE-2024-45558			
Buffer Over-read Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE Transient DOS can occur whether the driver parses the per STA profile IE and tries oduct/publicres ources/security bulletin/ianuary 200125						
when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/ianuary 200125					ion(s): -	Affected Vers
length.	UA-QCN6- 125/1332	alcomm.com/pr oduct/publicres ources/security bulletin/january	when the driver parses the per STA profile IE and tries to access the EXTN element	7.5	06-Jan-2025	
CVE ID: CVE-2024-45558 bulletin.html			CVE ID: CVE-2024-45558			
Product: qcn6224_firmware					16224_firmware	Product: qcr
Affected Version(s): -					ion(s): -	Affected Vers

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCN6- 200125/1333
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCN6- 200125/1334
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCN6- 200125/1335
Product: qc	n6274_firmware	<u> </u>			
Affected Vers	sion(s): -				
			Memory corruption can		
Use After Free	06-Jan-2025	7.8	occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCN6- 200125/1336
	06-Jan-2025 06-Jan-2025	7.8	maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
Product: qcr	16402_firmware	<u> </u>			
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCN6- 200125/1339
Product: qcr	16412_firmware	<u> </u>			
Affected Vers					
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCN6- 200125/1340
- 1	6.100 G		CVE ID: CVE-2024-45558	bulletin.html	
	16422_firmware	 			
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCN6- 200125/1341
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qcr	16432_firmware)			
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCN6- 200125/1342

4-5

5-6

6-7

8-9

9-10

7-8

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcn	7605_firmware	•			
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCN7- 200125/1343
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCN7- 200125/1344
Product: qcn	17606_firmware	;			
Affected Vers	ion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCN7- 200125/1345
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCN7- 200125/1346
Product: qcn	19000_firmware	•			
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCN9- 200125/1347
Product: qcn	19012_firmware	;			
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qu alcomm.com/pr oduct/publicres	0-QUA-QCN9- 200125/1348
CVSSv3 Scoring	Scale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-1
* stands for all v		1-2	3-4 4-3 5-6	0-7 /-0	9-1

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	ources/security bulletin/january -2025- bulletin.html	
Product: qcr	 19022_firmware	<u> </u>			
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCN9- 200125/1349
Product: qcr	19024_firmware	•			
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCN9- 200125/1350
Product: qcr	19070_firmware	<u> </u>			
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCN9- 200125/1351
D 1 .			CVE ID: CVE-2024-45558	bulletin.html	
	19072_firmware)			
Affected Vers	sion(s): -		Tuesdant DOC		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCN9- 200125/1352

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
de . 1 C 11 1										

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcr	19074_firmware	,			
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCN9- 200125/1353
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCN9- 200125/1354
D 1 .	0400 6		CVE ID: CVE-2024-33067	bulletin.html	
	19100_firmware	•			
Affected Vers Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCN9- 200125/1355
Product: qcr	19160_firmware	•			
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCN9- 200125/1356
Product: qcr	19274_firmware	·			
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCN9- 200125/1357

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qcs	410_firmware				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCS4- 200125/1358
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCS4- 200125/1359
Product: qcs	4490_firmware				
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCS4- 200125/1360
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCS4- 200125/1361
Product: qcs	5430_firmware				
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	0-QUA-QCS5- 200125/1362

0-1

4-5

5-6

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			CVE ID: CVE-2024-45541	-2025- bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCS5- 200125/1363
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCS5- 200125/1364
Duo du at. a aa	(10 firmyyana		CVE ID: CVE-2024-45558	bulletin.ntml	
•	610_firmware				
Affected Vers	1011(8): -		Transient DOS can occur		
Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCS6- 200125/1365
			CVE ID: CVE-2024-45558	bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QCS6- 200125/1366
			CVE ID: CVE-2024-33067	bulletin.html	
Product: qcs	6490_firmware				
Affected Vers	ion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCS6- 200125/1367
Buffer Copy without Checking Size of Input ('Classic	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	0-QUA-QCS6- 200125/1368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			CVE ID: CVE-2024-45541	-2025- bulletin.html	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCS6- 200125/1369
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCS6- 200125/1370
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCS6- 200125/1371
Product: qcs	7230_firmware				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCS7- 200125/1372
			CVE ID: CVE-2024-45553		
Product: qcs	8250_firmware				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCS8- 200125/1373

CVSSv3 Scoring Scale	
* stands for all version	s

5-6

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45553		
Product: qcs	8550_firmware				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCS8- 200125/1374
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCS8- 200125/1375
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. CVE ID: CVE-2024-33061	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCS8- 200125/1376
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCS8- 200125/1377
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QCS8- 200125/1378
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls,	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	0-QUA-QCS8- 200125/1379

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33041	-2025- bulletin.html	
Product: qo	s9100_firmware				
Affected Ver	rsion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QCS9- 200125/1380
Product: gc	 u1000_firmwar	e e			
Affected Ver					
Use After Free		7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QDU1- 200125/1381
Droduct, ac	lu1010 firmwan		0.2.2.0.2.2021		
	lu1010_firmwar	E			
Affected Ver	sion(s): -		La .		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QDU1- 200125/1382
D 1	1446		CVE ID: CVE-2024-45553		
	lu1110_firmwar	e			
Affected Ver	rsion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QDU1- 200125/1383

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using it for a process- specific task, issues may arise.	bulletin.html	
			CVE ID: CVE-2024-45553		
Product: qd	u1210_firmwar	e			
Affected Ver	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QDU1- 200125/1384
			CVE ID: CVE-2024-45553		
Product: qd	x1010_firmware	9			
Affected Ver	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QDX1- 200125/1385
			CVE ID: CVE-2024-45553		
Product: qd	x1011_firmward	9			
Affected Ver	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QDX1- 200125/1386
			CVE ID: CVE-2024-45553		
Product: qe	p8111_firmware	9			
	sion(s): -				

CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QEP8- 200125/1387
Product: afv	v7114_firmware	<u> </u>	CVL ID. CVL-2024-43333		
Affected Vers					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QFW7- 200125/1388
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QFW7- 200125/1389
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QFW7- 200125/1390
-	v7124_firmware	9			
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QFW7- 200125/1391

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific task, issues may arise.		
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QFW7- 200125/1392
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-QFW7- 200125/1393
	_		CVE ID: CVE-2024-33067	bulletin.html	
-	5165n_firmwar	·e			
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QRB5- 200125/1394
			CVE ID: CVE-2024-45553		
Product: qru	11032_firmware				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QRU1- 200125/1395
Product: qru	ı1052_firmware				

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product: qru1062 Affected Version(s) Product: qsm8256 Affected Version(s)	-Jan-2025 2_firmwar): -	7.8 e	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Memory corruption can occur when process-specific	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QRU1- 200125/1396
Product: qru1062 Affected Version(s) Product: qsm825 Affected Version(s) Buffer Over- 06-	2_firmware): -		occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Memory corruption can	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	
Affected Version(s) Use After Pree 06- Product: qsm825 Affected Version(s)): -	е			
Use After Free 06- Product: qsm825 Affected Version(s)					
Product: qsm8250 Affected Version(s) Buffer Over-					
Affected Version(s) Buffer Over-	-Jan-2025	7.8	maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QRU1- 200125/1397
Affected Version(s) Buffer Over-	0 G		CVL ID. CVL-2024-43333		
Buffer Over-		e			
	-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-QSM8- 200125/1398
Product: qxm808	3 firmwar	re			
Affected Version(s)					
Ruffer Over-	-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-QXM8- 200125/1399
Product: robotics	-jaii-2023				

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-ROBO- 200125/1400
Product: sa6	145p_firmware				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA61- 200125/1401
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA61- 200125/1402
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA61- 200125/1403
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA61- 200125/1404
Product: sa6	5150p_firmware				

0-1

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA61- 200125/1405
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA61- 200125/1406
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA61- 200125/1407
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA61- 200125/1408
Product: sa6	5155p_firmware	<u> </u>			
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA61- 200125/1409

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA61- 200125/1410
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA61- 200125/1411
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA61- 200125/1412
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA61- 200125/1413
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA61- 200125/1414
Product: sa6	155_firmware				
Affected Vers	ion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images,	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA61- 200125/1415

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabling the booting of a tampered IFS2 system image.		
			CVE ID: CVE-2024-45555		
Product: sa7	255p_firmware	<u> </u>			
Affected Vers	ion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA72- 200125/1416
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA72- 200125/1417
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-SA72- 200125/1418
			CVE ID: CVE-2024-45558	bulletin.html	
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA72- 200125/1419
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend.	https://docs.qu alcomm.com/pr oduct/publicres ources/security	0-QUA-SA72- 200125/1420

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID: CVE-2024-45559	bulletin/january -2025- bulletin.html				
Product: sa7775p_firmware								
Affected Vers	sion(s): -							
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA77- 200125/1421			
			CVE ID: CVE-2024-45555					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA77- 200125/1422			
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA77- 200125/1423			
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA77- 200125/1424			
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-SA77- 200125/1425			

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
				bulletin.html			
Product: sa8145p_firmware							
Affected Vers	ion(s): -						
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA81- 200125/1426		
			CVE ID: CVE-2024-45555				
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA81- 200125/1427		
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA81- 200125/1428		
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA81- 200125/1429		
D 1			CVE ID. CVE-2024-33007	buneum.num			
	3150p_firmware						
Affected Vers	ion(s): -						
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA81- 200125/1430		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45555		
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA81- 200125/1431
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA81- 200125/1432
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-SA81- 200125/1433
			CVE ID: CVE-2024-33067	bulletin.html	
	3155p_firmware				
Affected Vers	sion(s): -		Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification.	https://docs.qu	
Out-of- bounds Write	06-Jan-2025	8.4	This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA81- 200125/1434
bounds	06-Jan-2025	8.4	This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system	oduct/publicres ources/security bulletin/january -2025-	
bounds	06-Jan-2025 06-Jan-2025	7.8	This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	oduct/publicres ources/security bulletin/january -2025-	

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1436
			CVE ID: CVE-2024-45558		
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA81- 200125/1437
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA81- 200125/1438
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA81- 200125/1439
Product: sa8	3155_firmware				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA81- 200125/1440
Product: sa8	3195p_firmware				
Affected Vers	sion(s): -				
Out-of- bounds	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten,	https://docs.qu alcomm.com/pr oduct/publicres	0-QUA-SA81- 200125/1441

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA81- 200125/1442
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA81- 200125/1443
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA81- 200125/1444
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA81- 200125/1445
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-SA81- 200125/1446
			CVE ID: CVE-2024-33067	bulletin.html	

CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Vers	Affected Version(s): -							
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA82- 200125/1447			
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA82- 200125/1448			
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA82- 200125/1449			
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA82- 200125/1450			
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA82- 200125/1451			
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API.	https://docs.qu alcomm.com/pr oduct/publicres	0-QUA-SA82- 200125/1452			

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43063	ources/security bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-SA82- 200125/1453
			CVL ID. CVL 2024 43337	bulletin.html	
	3295p_firmware	:			
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA82- 200125/1454
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA82- 200125/1455
			CVE ID: CVE-2024-45553		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA82- 200125/1456
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-SA82- 200125/1457

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558	bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA82- 200125/1458
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA82- 200125/1459
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA82- 200125/1460
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA82- 200125/1461
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA82- 200125/1462
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA82- 200125/1463
	3530p_firmware	;			
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qu alcomm.com/pr oduct/publicres	0-QUA-SA85- 200125/1464

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	ources/security bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA85- 200125/1465
Product: sa8	3540p_firmware				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA85- 200125/1466
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA85- 200125/1467
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA85- 200125/1468
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA85- 200125/1469

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA85- 200125/1470
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA85- 200125/1471
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA85- 200125/1472
Product: sa8	3620p_firmware				l
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA86- 200125/1473
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA86- 200125/1474
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU	https://docs.qu alcomm.com/pr oduct/publicres	0-QUA-SA86- 200125/1475

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	ources/security bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA86- 200125/1476
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA86- 200125/1477
Product: sa8	8650p_firmware			bunetiii.iitiiii	
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA86- 200125/1478
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA86- 200125/1479
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	0-QUA-SA86- 200125/1480

CVSSv3 Scoring Scale
* stands for all versions

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length. CVE ID: CVE-2024-45558	-2025- bulletin.html	
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA86- 200125/1481
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA86- 200125/1482
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA86- 200125/1483
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA86- 200125/1484
Product: sa8	3770p_firmware			banetiiiiii	
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA87- 200125/1485
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is	https://docs.qu alcomm.com/pr oduct/publicres ources/security	0-QUA-SA87- 200125/1486

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removed from the global list while another thread is using it for a process- specific task, issues may arise.	bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45553		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-SA87- 200125/1487
			CVE ID: CVE-2024-43064	bulletin.html	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-SA87- 200125/1488
			CVE ID: CVE-2024-45558	bulletin.html	
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA87- 200125/1489
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA87- 200125/1490
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA87- 200125/1491
Product: sa8	3775p_firmware				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification.	https://docs.qu alcomm.com/pr oduct/publicres ources/security	0-QUA-SA87- 200125/1492

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA87- 200125/1493
			CVE ID: CVE-2024-45553		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA87- 200125/1494
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA87- 200125/1495
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA87- 200125/1496
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA87- 200125/1497
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific	https://docs.qu alcomm.com/pr	0-QUA-SA87- 200125/1498

CVSSv3 Scoring Scale
* stands for all versions

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message type to the Vdev- FastRPC backend. CVE ID: CVE-2024-45559	oduct/publicres ources/security bulletin/january	
			CVL ID. CVL-2024-43337	-2025- bulletin.html	
	0000p_firmware	<u> </u>			
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA90- 200125/1499
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA90- 200125/1500
			CVE ID: CVE-2024-45553		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-SA90- 200125/1501
			CVE ID: CVE-2024-43064	bulletin.html	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SA90- 200125/1502
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger	https://docs.qu alcomm.com/pr oduct/publicres ources/security	0-QUA-SA90- 200125/1503

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than mailbox size. CVE ID: CVE-2024-23366	bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA90- 200125/1504
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA90- 200125/1505
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SA90- 200125/1506
Product: sc8	180x-aaab_firm	ware		Suitetimiem	
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-SC81- 200125/1507
Overflow') Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SC81- 200125/1508
Product: sc8	180x-acaf_firm	ware			
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-SC81- 200125/1509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')	22011 2400		p	bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SC81- 200125/1510
Product: sc8	180x-ad_firmwa	are			
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SC81- 200125/1511
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SC81- 200125/1512
Product: sc8	180xp-aaab_fir	mware			
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SC81- 200125/1513
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SC81- 200125/1514
Product: sc8	180xp-acaf_firn	nware			
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-SC81- 200125/1515

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')	_ 45234 2460	2.22.3		bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SC81- 200125/1516
Product: sc8	180xp-ad_firmv	vare			
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SC81- 200125/1517
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SC81- 200125/1518
Product: sc8	180x\+sdx55_fi	rmware			
Affected Vers	sion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SC81- 200125/1519
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SC81- 200125/1520
Product: sc8	280xp-abbb_fir	mware			
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-SC82- 200125/1521

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')				bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SC82- 200125/1522
Product: sc8	380xp_firmwar	e			
Affected Vers	sion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SC83- 200125/1523
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SC83- 200125/1524
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SC83- 200125/1525
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SC83- 200125/1526
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. CVE ID: CVE-2024-45550	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SC83- 200125/1527
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call.	https://docs.qu alcomm.com/pr oduct/publicres ources/security	0-QUA-SC83- 200125/1528

CVSSv3 Scoring Scale
* stands for all versions

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45548	bulletin/january -2025- bulletin.html	
Product: sd8	335_firmware				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SD83- 200125/1529
Product: sd8	865_5g_firmwar	e			
Affected Vers					
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SD86- 200125/1530
Product: sdr	n429w_firmwar	·e			
Affected Vers	ion(s): -				
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SDM4- 200125/1531
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SDM4- 200125/1532
Product: sdx	55_firmware				
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qu alcomm.com/pr oduct/publicres	0-QUA-SDX5- 200125/1533

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	ources/security bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SDX5- 200125/1534
Product: sdx	x65m_firmware				
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-SDX6- 200125/1535
			CVE ID: CVE-2024-45558	bulletin.html	
	8_gen1_5g_firm	ware			
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SD_8- 200125/1536
			CVE ID: CVE-2024-45553		
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SD_8- 200125/1537
	150p_firmware				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific	https://docs.qu alcomm.com/pr	0-QUA-SG41- 200125/1538

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
Dwo dwat, ag	275 firming		CVE ID: CVE-2024-45555		
Affected Vers	3275p_firmware				
Affected vers	51011(5)		Mamagra garmentian suban	hu - //l	
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SG82- 200125/1539
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SG82- 200125/1540
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SG82- 200125/1541
Product: sm	4635_firmware				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SM46- 200125/1542
			CVE ID: CVE-2024-45553		
Product: sm	6250_firmware				
Affected Vers	sion(s): -				

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
aveeve beening beare	0 1		_ 0	0 1	1 0	0 0	0 ,	, 0	0 /	7 10

^{*} stands for all versions

Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') Stack-based		7.8 7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541 Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SM62- 200125/1543 O-QUA-SM62- 200125/1544
without Checking Size of Input ('Classic Buffer Overflow') Stack-based Buffer Overflow Product: sm665	06-Jan-2025 50_firmware		IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541 Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	200125/1543 O-QUA-SM62-
Buffer 0 Overflow Product: sm665	50_firmware	7.8	IOCTL call is invoked from user-space to write board data to WLAN driver.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	· ·
Affected Version	ı(s): -				
Use After Free 0	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SM66- 200125/1545
Buffer Over- read 0	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SM66- 200125/1546
Product: sm763	35_firmware				l
Affected Version	n(s): -				
Use After Free 0	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SM76- 200125/1547
Buffer Over- 0	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	O-QUA-SM76-

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1548
			CVE ID: CVE-2024-45558	bunetiii.iitiiii	
Product: sm	7675p_firmwar	e			
Affected Vers	ion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SM76- 200125/1549
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-SM76- 200125/1550
			CVE ID: CVE-2024-45558	bulletin.html	
Product: sm	7675_firmware				
Affected Vers	ion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SM76- 200125/1551
Buffer Over- read	06-Jan-2025	7.5	CVE ID: CVE-2024-45553 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SM76- 200125/1552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sm	8550p_firmwar	e			
Affected Vers	ion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SM85- 200125/1553
			Transient DOS can occur	1 //1	
Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SM85- 200125/1554
				https://docs.qu	
Use After Free 06-Ja	06-Jan-2025	06-Jan-2025 6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SM85- 200125/1555
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SM85- 200125/1556
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-SM85- 200125/1557
Product: cm	8635p_firmwar	P	5.2 1D. 5.1 2021-33011	bulletin.html	
Affected Vers					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	0-QUA-SM86- 200125/1558
CUCC. 2 C	Cl- 0.4	1.2			0.0
* stands for all v		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-1

Product: sm8635_firmware Affected Version(s): - Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 D-QUA-SM86-200125/1560 D-QUA-SM86-200125/1560 D-QUA-SM86-200125/1560 D-QUA-SM86-200125/1560 D-QUA-SM86-200125/1561	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over- read 06-Jan-2025 7.5 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Delletin.html DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Delletin.html				using it for a process- specific task, issues may arise.		
Buffer Over- read 06-Jan-2025 7.5 when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 bulletin.html Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using if for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 bulletin.html Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 bulletin.html Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 bulletin.html Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 bulletin.html Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 bulletin.html Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 bulletin.html Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 bulletin.html				CVE ID: CVE-2024-45553		
Affected Version(s): - Joe	Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	•
Affected Version(s): - Joe	Product: sm	8635 firmware				
Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Product: sm8750p_firmware 7.5 Buffer Over-read O6-Jan-2025 O6-Jan-2025 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 CVE ID: CVE-2024-45558 CVE ID: CVE-2024-45558 Product: sm8750_firmware						
Buffer Over- read 06-Jan-2025 7.5 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 D-QUA-SM87-200125/1562 D-QUA-SM87-200125/1562 D-QUA-SM87-200125/1562 D-QUA-SM87-200125/1562			7.8	occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	
Affected Version(s): - Buffer Over- read O6-Jan-2025 7.5 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries oduct/publicres ources/security bulletin/january -2025-bulletin.html	Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	
Buffer Over-read O6-Jan-2025 7.5 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 CVE ID: CVE-2024-45558 Transient DOS can occur when the driver parses the per STA profile IE and tries oduct/publicres ources/security bulletin/january -2025-bulletin.html	Product: sm	8750p_firmwar	e			l
Buffer Over-read 06-Jan-2025 7.5 when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 when the driver parses the per STA profile IE and tries oduct/publicres ources/security bulletin/january -2025-bulletin.html	Affected Vers	ion(s): -				
	Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	
	Product: sm	8750_firmware				
THE COLUMN TO A STATE OF THE ST						

CVSSv3 Scoring Scale	0-1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	---------	-----	-----	-----	-----	-----	-----	-----	------

Weelmag	Dublish Data	CVCC2	Description & CVE ID	Dotak	NCHDC ID
Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-SM87- 200125/1563
	_		CVE ID: CVE-2024-45558	bulletin.html	
	npdragon_429_n	nobile_fir	mware		
Affected Vers	sion(s): -				
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SNAP- 200125/1564
			Information disclosure		
Buffer Over- read	06-Jan-2025	6.1	while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-SNAP- 200125/1565
			CVE ID: CVE-2024-33067	bulletin.html	
Product: sna	npdragon_460_n	nobile_fir	mware		
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SNAP- 200125/1566
			CVE ID: CVE-2024-45553		
Product: sna	apdragon_480\+	5g_mob	ile_firmware		
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-SNAP- 200125/1567

CVSSv3 Scoring Scale
* stands for all versions

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using it for a process- specific task, issues may arise.	bulletin.html	
			CVE ID: CVE-2024-45553		
Product: sn	apdragon_480_5	g_mobile	_firmware		
Affected Ver	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SNAP- 200125/1568
			CVE ID: CVE-2024-45553		
Product: sn	apdragon_4_gen	_1_mobile	e_firmware		
Affected Ver	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SNAP- 200125/1569
			CVE ID: CVE-2024-45553		
Product: sn	apdragon_4_gen	_2_mobile	e_firmware		
Affected Ver	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SNAP- 200125/1570
			CVE ID: CVE-2024-45553		
Product: sn	apdragon_662_n	nobile_fir	mware		

CVSSv3 Scoring Scale	0-1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	---------	-----	-----	-----	-----	-----	-----	-----	------

Maalw	m 0.00	Dublish Data	CVCC2	Decomination & CVE ID	Datah	NCHDC ID
Weak	ness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use Free	After	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SNAP- 200125/1571
Prodi	ıct: sna	npdragon_680_4	g mohile			
		sion(s): -	g_mobile,			
Allect	eu vers	1011(8): -				
Use Free	After	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SNAP- 200125/1572
				CVE ID: CVE-2024-45553		
Produ	ıct: sna	pdragon_685_4	g_mobile	_firmware		
Affect	ed Vers	sion(s): -				
Use Free	After	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1573
				CVE ID: CVE-2024-45553		
Produ	ıct: sna	pdragon_695_5	g_mobile	_firmware		
		sion(s): -				
Use Free	After	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1574

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45553		
Product: sna	pdragon_7c\+_	gen_3_cor	npute_firmware		
Affected Vers	ion(s): -		•		
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1575
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1576
Product: sna	pdragon_7c_co	mpute_pl	atform_firmware		
Affected Vers	ion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1577
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1578
	pdragon_7c_ge	n_2_comp	ute_platform_firmware	1	<u>'</u>
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SNAP- 200125/1579
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	O-QUA-SNAP- 200125/1580
* stands for all v		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-1

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45542	-2025- bulletin.html	
Product: sna	apdragon_820_a	utomotiv	e_firmware		
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SNAP- 200125/1581
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1582
Product: sna	npdragon_835_n	nobile_pc	_firmware		
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1583
Product: sna	npdragon_865\+	5g_mob	ile_firmware		
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1584
Product: sna	 apdragon_865_5	g mobile	firmware		
Affected Vers		9_1100110			
miccieu veis	non(s)				

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1585
Product: sna	pdragon_870_5	g mobile	firmware		
Affected Vers		6	-		
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-SNAP- 200125/1586
			CVE ID: CVE-2024-33067	bulletin.html	
Product: sna	pdragon_8\+_g	en_1_mob	oile_firmware		
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1587
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SNAP- 200125/1588
Product: sna	pdragon_8\+_g	en 2 mob	l pile firmware		
Affected Vers					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arise.		
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1590
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1591
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1592
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1593
Product: sn	apdragon_8_gen	_1_mobile	e_firmware		
Affected Ver	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1594
D 1 .	 apdragon_8_gen	_2_mobile	e_firmware		
Product: sn					
Affected Ver	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1596
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1597
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1598
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1599
Product: sna	npdragon_8_gen	_3_mobile	e_firmware		
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SNAP- 200125/1600
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the	https://docs.qu alcomm.com/pr oduct/publicres	0-QUA-SNAP- 200125/1601

CVSSv3 Scoring Scale
* stands for all versions

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global list. If a map is removed from the global list while another thread is using it for a process- specific task, issues may arise.	ources/security bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1602
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SNAP- 200125/1603
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1604
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1605
Product: sna	ipdragon_ar1_g	en_1_firm	ware		
Affected Vers	ion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1606
			CVE ID: CVE-2024-45553		

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sna	pdragon_ar2_g	en_1_firm	ware		
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1607
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1608
Product: sna	pdragon_auto_	4g_moder	n_firmware		
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1609
Product: sna	pdragon_auto_!	5g_moder	n-rf_gen_2_firmware		
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SNAP- 200125/1610
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	O-QUA-SNAP- 200125/1611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length. CVE ID: CVE-2024-45558	-2025- bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-SNAP- 200125/1612
			CVE ID: CVE-2024-33067	bulletin.html	
Product: sna	apdragon_w5\+_	_gen_1_we	earable_firmware		
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1613
			CVE ID: CVE-2024-45553		
Product: sna	apdragon_x35_5	g_modem	ı-rf_firmware		
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1614
Duo du eti ene	ndragan v.F.F. F	a madam			
	apdragon_x55_5	g_modem	i-ri_mmware		
Affected Vers	sion(s): -		Information		
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1615

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sna	npdragon_x65_5	g modem	-		
Affected Vers		<u> </u>			
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SNAP- 200125/1616
Product: sna	npdragon_x72_5	g_modem	-rf_firmware		
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SNAP- 200125/1617
			CVE ID: CVE-2024-45553 Transient DOS can occur	https://docs.qu	
Buffer Over- read	06-Jan-2025	7.5	when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SNAP- 200125/1618
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1619
Product: sna	pdragon_x75_5	g_modem	-rf_firmware		
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-SNAP- 200125/1620

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using it for a process- specific task, issues may arise.	bulletin.html	
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SNAP- 200125/1621
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-SNAP- 200125/1622
			CVE ID: CVE-2024-33067	bulletin.html	
Product: sna	npdragon_xr2_5	g_firmwa	re		
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-SNAP- 200125/1623
D 1 .	4) 6		CVE ID: CVE-2024-33067	bulletin.html	
	1h_firmware				
Affected Vers	sion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SRV1- 200125/1624
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the	https://docs.qu alcomm.com/pr oduct/publicres	0-QUA-SRV1- 200125/1625

CVSSv3 Scoring Scale
* stands for all versions

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global list. If a map is removed from the global list while another thread is using it for a process- specific task, issues may arise.	ources/security bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45553		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-SRV1- 200125/1626
			CVE ID: CVE-2024-43064	bulletin.html	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-SRV1- 200125/1627
			CVE ID: CVE-2024-45558	bulletin.html	
Buffer Over- read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. CVE ID: CVE-2024-23366	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-SRV1- 200125/1628
Buffer Over- read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. CVE ID: CVE-2024-43063	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SRV1- 200125/1629
Buffer Over- read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SRV1- 200125/1630
Product: srv	1l_firmware				
Affected Vers	ion(s): -				
Out-of- bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten,	https://docs.qu alcomm.com/pr oduct/publicres	0-QUA-SRV1- 200125/1631

4-5

5-6

6-7

3-4

2-3

8-9

9-10

		bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	ources/security bulletin/january -2025- bulletin.html	
		CVE ID: CVE-2024-45555		
06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SRV1- 200125/1632
06-Jan-2025	7.5	consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SRV1- 200125/1633
06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SRV1- 200125/1634
06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SRV1- 200125/1635
1m_firmware				
ion(s): -				
06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	0-QUA-SRV1- 200125/1636
	06-Jan-2025 06-Jan-2025 1m_firmware ion(s): -	06-Jan-2025 7.5 06-Jan-2025 5.5 1m_firmware ion(s): -	enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555 Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559 Im_firmware ion(s):- Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification.	enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555 Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	-2025- bulletin.html	
		Memory corruption can		
06-Jan-2025	7.8	occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process- specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SRV1- 200125/1637
		CVE ID: CVE-2024-45553		
06-Jan-2025	5 7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SRV1- 200125/1638
		CVE ID: CVE-2024-45558		
06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SRV1- 200125/1639
06-Jan-2025	5.5	when GVM sends a specific message type to the Vdev-FastRPC backend.	alcomm.com/pr oduct/publicres ources/security bulletin/january	0-QUA-SRV1- 200125/1640
044E C		0.11.0.11.0.11	bulletin.html	
• -	е			
1011(3).		Memory corruption can	https://docs.gu	
06-Jan-2025	7.8	occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SSG2- 200125/1641
	06-Jan-2025 06-Jan-2025 06-Jan-2025 2115p_firmwar	06-Jan-2025 7.8 06-Jan-2025 7.5 06-Jan-2025 5.5 2115p_firmware sion(s): -	programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555 Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064 Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559 Z115p_firmware cion(s):- Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is	programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. CVE ID: CVE-2024-45555 Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553 Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558 Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064 Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559 2115p_firmware ion(s): Memory corruption can occur when GVM sends a specific message type to the Vdev-FastRPC backend. CVE ID: CVE-2024-45559 2115p_firmware ion(s): Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is unled in the product/publicres ources/security bulletin/january -2025-bulletin.html

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific task, issues may arise.		
			CVE ID: CVE-2024-45553		
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SSG2- 200125/1642
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SSG2- 200125/1643
Product: ssg	2125p_firmwar	е			
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SSG2- 200125/1644
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SSG2- 200125/1645
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SSG2- 200125/1646
Product: sw	5100p_firmwar	e			
Affected Vers	sion(s): -				
Use After		7.8	Memory corruption can	https://docs.qu	0-QUA-SW51-

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-SW51- 200125/1648
			CVE ID: CVE-2024-33061	bulletin.html	
Product: sw	5100_firmware				
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SW51- 200125/1649
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-SW51- 200125/1650
			CVE ID: CVE-2024-33061	bulletin.html	
Product: sxr	1230p_firmwar	e			
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SXR1- 200125/1651

4-5

5-6

6-7

7-8

9-10

3-4

	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45553		
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SXR1- 200125/1652
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SXR1- 200125/1653
Product: sxr2	2130_firmware			Dunetiii.iitiiii	
Affected Versi	ion(s): -				
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SXR2- 200125/1654
Product: sxr2	2230p_firmwar	e			
Affected Versi	ion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SXR2- 200125/1655
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SXR2- 200125/1656
Use After	06-Jan-2025	6.7	Memory corruption while	https://docs.qu	O-QUA-SXR2-

CVSSv3 Scoring Scale
* stands for all versions 0-1 2-3 3-4 5-6 6-7 7-8 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Free			invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1657
Product: sxr	2250p_firmwar	'e		bunetiii.iitiiii	
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SXR2- 200125/1658
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-SXR2- 200125/1659
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SXR2- 200125/1660
Product: sxr	2330p_firmwar	e			
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-SXR2- 200125/1661
Product: tal	ynplus_firmwar	e			
Affected Vers	•				
Buffer Copy	06-Jan-2025	8.4	Memory corruption while	https://docs.qu	O-QUA-TALY-
Danci Copy	00 jan 2023	0.1	Mine wille	incepsif / doesiqu	o gon indi-

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1662
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-TALY- 200125/1663
D J		1 C	CVE ID: CVE-2024-45553		
	eo_collaboratio	n_vc1_firi	mware 		
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-VIDE- 200125/1664
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-VIDE- 200125/1665
Product: vid	eo_collaboratio	n_vc3_firi	l mware		
Affected Vers					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-VIDE- 200125/1666
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	0-QUA-VIDE- 200125/1667

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45542	-2025- bulletin.html	
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-VIDE- 200125/1668
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-VIDE- 200125/1669
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-VIDE- 200125/1670
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-VIDE- 200125/1671
Product: vid	eo_collaboratio	n_vc5_fir	nware		
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-VIDE- 200125/1672
D 1	1000 = 6		CVE ID: CVE-2024-45553		
	d9335_firmwar	e			
Affected Vers Buffer Over-		6.1	Information disclosure	https://dogs.go	O OHA WCDO
buller Over-	06-Jan-2025	0.1	Information disclosure	https://docs.qu	O-QUA-WCD9-

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read	- ususii sutt	5.3373	while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1673
Product: wc	d9340_firmwar	e			
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1674
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1675
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WCD9- 200125/1676
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1677
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WCD9- 200125/1678

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wc	d9341_firmwar	e			
Affected Vers	ion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WCD9- 200125/1679
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1680
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1681
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WCD9- 200125/1682
Product: wc	d9370_firmwar	e			
Affected Vers					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1683
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1684
Buffer Copy	06-Jan-2025	7.8	Memory corruption when	https://docs.qu	O-QUA-WCD9-

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1685
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1686
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1687
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-WCD9- 200125/1688
			CVE ID: CVE-2024-33067	bulletin.html	
Product: wc	d9375_firmwar	e			
Affected Vers	ion(s): -				
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1689
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1690
Use After	06-Jan-2025	7.8	Memory corruption can	https://docs.qu	O-QUA-WCD9-

0-1

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Free			occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1691
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1692
Product: wc	d9378_firmwar	Δ	CVE ID: CVE-2024-45556	buneum.num	
Affected Vers					
Affected vers	1011(3)				Г
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WCD9- 200125/1693
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-WCD9- 200125/1694
			CVE ID: CVE-2024-45558	bulletin.html	
Product: wc	d9380_firmwar	e			
Affected Vers	sion(s): -				
			Memory corruption while processing FIPS encryption or decryption IOCTL call	https://docs.qu alcomm.com/pr oduct/publicres ources/security	O-QUA-WCD9-
Buffer Over- read	06-Jan-2025	7.8	invoked from user-space. CVE ID: CVE-2024-45546	bulletin/january -2025- bulletin.html	200125/1695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1696
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. CVE ID: CVE-2024-45548	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WCD9- 200125/1697
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. CVE ID: CVE-2024-45550	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WCD9- 200125/1698
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WCD9- 200125/1699
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WCD9- 200125/1700
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1701
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	0-QUA-WCD9- 200125/1702

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length. CVE ID: CVE-2024-45558	-2025- bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1703
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1704
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-WCD9- 200125/1705
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1706
Due des ets sues	10205 G		CVL 1D. CVL 2021 33007	buneem.nem	
Affected Vers	d9385_firmwar	e 			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1707
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1708
Use After	06-Jan-2025	7.8	Memory corruption can	https://docs.qu	O-QUA-WCD9-

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WCD9- 200125/1710
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1711
				https://docs.qu	
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. CVE ID: CVE-2024-45548	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WCD9- 200125/1712
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. CVE ID: CVE-2024-45550	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WCD9- 200125/1713
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WCD9- 200125/1714
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls,	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	0-QUA-WCD9- 200125/1715

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33041	-2025- bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1716
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1717
Product: wc	d9390_firmwar	e			
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1718
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1719
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1720
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-WCD9- 200125/1721

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			-	bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1722
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1723
Product: wc	d9395_firmwar	e			
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1724
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1725
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1726
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1727

5-6

6-7

7-8

9-10

3-4

XAZ a alam a a a	Dublish Data	CVCC2	Description 0 CVF ID	Datah	NCHDC ID
Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1728
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCD9- 200125/1729
Product: wc	n3620_firmwar	e			
Affected Vers	sion(s): -				
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-WCN3- 200125/1730
			CVE ID: CVE-2024-43064	bulletin.html	
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-WCN3- 200125/1731
			CVE ID: CVE-2024-33067	bulletin.html	
Product: wc	n3660b_firmwa	re			<u> </u>
Affected Vers	sion(s): -				
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. CVE ID: CVE-2024-43064	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCN3- 200125/1732
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCN3- 200125/1733

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33061		
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCN3- 200125/1734
Product: wc	 n3680b_firmwa	re	CVE 1D. CVE 2021 33007	buncummum	
Affected Vers					
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. CVE ID: CVE-2024-33061	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCN3- 200125/1735
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCN3- 200125/1736
Product: wc	n3950_firmwar	e e			
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-WCN3- 200125/1737
Overflow') Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCN3- 200125/1738

CVSSv3 Scoring Scale	0-1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	---------	-----	-----	-----	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakiless	r ublish Date	CV33V3	-	rattii	NCIIFCID
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCN3- 200125/1739
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCN3- 200125/1740
Product: wc	n3980_firmwar	e			
Affected Vers	sion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCN3- 200125/1741
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. CVE ID: CVE-2024-33061	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WCN3- 200125/1742
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCN3- 200125/1743
Product: wc	n3988_firmwar	e			
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is	https://docs.qu alcomm.com/pr oduct/publicres ources/security	0-QUA-WCN3- 200125/1744

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removed from the global list while another thread is using it for a process- specific task, issues may arise.	bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCN3- 200125/1745
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. CVE ID: CVE-2024-33061	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WCN3- 200125/1746
Product: wc	n3990_firmwar	e e			
Affected Vers					
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-WCN3- 200125/1747
			CVE ID: CVE-2024-33067	bulletin.html	
	n6450_firmwar	е			
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCN6- 200125/1748
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the	https://docs.qu alcomm.com/pr	0-QUA-WCN6- 200125/1749

0-1

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			per STA profile IE and tries to access the EXTN element ID without checking the IE length.	oduct/publicres ources/security bulletin/january -2025-	
			CVE ID: CVE-2024-45558	bulletin.html	
Product: wc	n6650_firmwar	e			
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCN6- 200125/1750
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-WCN6- 200125/1751
			CVE ID: CVE-2024-45558	bulletin.html	
Product: wc	n6740_firmwar	е			
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january	0-QUA-WCN6- 200125/1752
Buffer Overflow')			CVE ID: CVE-2024-21464	-2025- bulletin.html	
	n6755_firmwar	e		- Sunctinitiiii	<u> </u>
Affected Vers	sion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCN6- 200125/1753

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCN6- 200125/1754
Product: wc	n7860_firmwar	e			
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-WCN7- 200125/1755
			CVE ID: CVE-2024-45558	bulletin.html	
Product: wc	n7861_firmwar	e			
Affected Vers	ion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCN7- 200125/1756
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WCN7- 200125/1757
Product: wci	n7880_firmwar	e			
Affected Vers	ion(s): -				
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element	https://docs.qu alcomm.com/pr oduct/publicres ources/security	O-QUA-WCN7- 200125/1758

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID without checking the IE length.	bulletin/january	
			CVE ID: CVE-2024-45558	bulletin.html	
Product: wci	n7881_firmwar	e			
Affected Vers	ion(s): -				
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WCN7- 200125/1759
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WCN7- 200125/1760
Product: wsa	a8810_firmward	a			
Affected Vers					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1761
Use After	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-WSA8- 200125/1762
Free			arise. CVE ID: CVE-2024-45553	bulletin.html	
Buffer Copy without Checking Size of Input	06-Jan-2025	7.8	arise.		0-QUA-WSA8- 200125/1763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			CVE ID: CVE-2024-45541	bulletin/january -2025- bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1764
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1765
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-WSA8- 200125/1766
Due du et	-0015 G		CVE ID: CVE-2024-33067	bulletin.html	
	a8815_firmwar	e 			
Affected Vers	sion(s): -	ı			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1767
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1768
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1769
Use After	06-Jan-2025	7.8	Memory corruption can	https://docs.qu	O-QUA-WSA8-

CVSSv3 Scoring Scale
* stands for all versions

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Free			occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1770
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1771
Buffer Over- read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. CVE ID: CVE-2024-33067	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1772
Product: ws:	a8830_firmwar	p.	CVE 1D. CVE 2021 33007	bancanin	
Affected Vers					
Buffer Copy	ron(o).		Manager communication while	https://docs.qu	
without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1773
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1774
Duffer C				https://do	
Buffer Copy without Checking Size of Input	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data.	https://docs.qu alcomm.com/pr oduct/publicres ources/security	0-QUA-WSA8- 200125/1775

CVSSv3 Scoring Scale
* stands for all versions

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			CVE ID: CVE-2024-45541	bulletin/january -2025- bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1776
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1777
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. CVE ID: CVE-2024-33061	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1778
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1779
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1780
Product: ws:	a8832_firmwar	e			
Affected Vers	ion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1781
OVCITION				1	<u> </u>

CVSSv3 Scoring Scale
* stands for all versions

5-6

6-7

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Free			occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process- specific task, issues may arise.	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1782
			CVE ID: CVE-2024-45553		
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1783
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1784
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1785
Product: wsa	a8835_firmware	<u> </u>		Dunetin.ntim	
Affected Vers					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1786
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1787
Stack-based Buffer	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from	https://docs.qu alcomm.com/pr	0-QUA-WSA8- 200125/1788

0-1

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow			user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1789
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1790
Buffer Over- read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. CVE ID: CVE-2024-33061	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1791
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1792
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1793
	18840_firmwar	9			
Affected Vers Buffer Copy		0.4	Memory corruption while	https://docs.qu	O-QUA-WSA8-
without	06-Jan-2025	8.4	processing IPA statistics,	alcomm.com/pr	200125/1794
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			when there are no active clients registered. CVE ID: CVE-2024-21464	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1795
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	0-QUA-WSA8- 200125/1796
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. CVE ID: CVE-2024-45548	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1797
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. CVE ID: CVE-2024-45550	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1798
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1799
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025-	O-QUA-WSA8- 200125/1800

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')				bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1801
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1802
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1803
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1804
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1805
	a8845h_firmwa	re			
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1806
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is	https://docs.qu alcomm.com/pr oduct/publicres ources/security	0-QUA-WSA8- 200125/1807

CVSSv3 Scoring Scale
* stands for all versions

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removed from the global list while another thread is using it for a process- specific task, issues may arise.	bulletin/january -2025- bulletin.html	
			CVE ID: CVE-2024-45553		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1808
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1809
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1810
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1811
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. CVE ID: CVE-2024-45548	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1812
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. CVE ID: CVE-2024-45550	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1813
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	O-QUA-WSA8-

5-6

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	200125/1814
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1815
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. CVE ID: CVE-2024-33059	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1816
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1817
Product: ws	a8845_firmwar	e			
Affected Vers	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. CVE ID: CVE-2024-21464	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1818
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. CVE ID: CVE-2024-45553	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1819
Buffer Copy without	06-Jan-2025	7.8	Memory corruption while processing IOCTL call	https://docs.qu alcomm.com/pr	0-QUA-WSA8- 200125/1820

0-1

4-5

5-6

6-7

3-4

2-3

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			invoked from user-space to verify non extension FIPS encryption and decryption functionality. CVE ID: CVE-2024-45547	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. CVE ID: CVE-2024-45546	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1821
Buffer Over- read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. CVE ID: CVE-2024-45548	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1822
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. CVE ID: CVE-2024-45550	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1823
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. CVE ID: CVE-2024-45541	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1824
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. CVE ID: CVE-2024-45542	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1825
Buffer Over- read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. CVE ID: CVE-2024-45558	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1826
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command	https://docs.qu alcomm.com/pr	0-QUA-WSA8- 200125/1827

0-1

4-5

5-6

6-7

8-9

7-8

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL calls. CVE ID: CVE-2024-33059	oduct/publicres ources/security bulletin/january -2025- bulletin.html	
Use of Out- of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, CVE ID: CVE-2024-33041	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	0-QUA-WSA8- 200125/1828
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. CVE ID: CVE-2024-33055	https://docs.qu alcomm.com/pr oduct/publicres ources/security bulletin/january -2025- bulletin.html	O-QUA-WSA8- 200125/1829