

National Critical Information Infrastructure Protection Centre Common Vulnerabilities and Exposures (CVE) Report

01 - 15 Dec 2024

Vol. 11 No. 23

Table of Content			
Vendor	Product	Page Number	
Application			
	attendance_tracking_management_system	1	
1000projects	beauty_parlour_management_system	1	
	library_management_system	2	
	bridge	2	
	experience_manager	3	
Adobe	framemaker	27	
Auobe	premiere_pro	28	
	substance_3d_modeler	28	
	substance_3d_painter	31	
anisha	farmacia	32	
anujk305	medical_card_generation_system	32	
Apple	safari	32	
cjbi	wetech-cms	37	
classcms	classcms	43	
codo projecto	admin_dashboard	43	
code-projects	hotel_management_system	44	
codezips	technical_discussion_forum	45	
datax-web_project	datax-web	46	
Dedecms	dedecms	46	
fabian	online_class_and_exam_scheduling_system	48	
fabianros	online_notice_board	50	
GFI	archiver	50	
Google	chrome	52	
gstreamer_project	gstreamer	53	
IBM	cognos_controller	54	
ivanti	automation	63	
ivanti	security_controls	63	

Vendor	Product	Page Number
ivanti	workspace_control	64
jwillber	jfinalcms	64
lopalopa	e-learning_management_system	65
mayurik	advocate_office_management_system	68
mayurix	best_house_rental_management_system	68
online_class_and_exam_s cheduling_system_projec t	online_class_and_exam_scheduling_system	69
openrobotics	robot_operating_system	69
phpgurukul	complaint_management_system	72
րորքայառա	covid_19_testing_management_system	73
Progress	whatsup_gold	73
razormist	phone_contact_manager_system	75
Rockwellautomation	arena_simulation	77
ujcms	ujcms	78
Hardware		
	205_mobile_platform	78
	215_mobile_platform	79
	315_5g_iot_modem	79
	9205_lte_modem	80
	9206_lte_modem	80
	9207_lte_modem	81
	apq8017	81
	apq8037	82
Qualcomm	aqt1000	82
	ar8035	83
	c-v2x_9150	83
	csrb31024	84
	fastconnect_6200	85
	fastconnect_6700	86
	fastconnect_6800	88
	fastconnect_6900	90
	fastconnect_7800	94

Vendor	Product	Page Number
	flight_rb5_5g_platform	97
	fsm10055	98
	fsm10056	98
	home_hub_100_platform	99
	immersive_home_214_platform	99
	immersive_home_216_platform	100
	immersive_home_316_platform	100
	immersive_home_318_platform	100
	immersive_home_3210_platform	101
	immersive_home_326_platform	101
	ipq5010	102
	ipq5028	102
	ipq5300	103
	ipq5302	103
	ipq5312	104
Qualcomm	ipq5332	105
Qualcomm	ipq6000	105
	ipq6005	106
	ipq6010	106
	ipq6018	106
	ipq6028	107
	ipq8064	107
	ipq8065	107
	ipq8068	108
	ipq8070	108
	ipq8070a	108
	ipq8071	109
	ipq8071a	109
	ipq8072	110
	ipq8072a	110
	ipq8074	110
	ipq8074a	111

Vendor	Product	Page Number
	ipq8076	111
	ipq8076a	111
	ipq8078	112
	ipq8078a	112
	ipq8173	113
	ipq8174	113
	ipq9008	113
	ipq9554	114
	ipq9570	115
	ipq9574	115
	mdm8207	116
	mdm9205s	116
	mdm9250	117
	mdm9628	117
	mdm9650	117
Qualcomm	msm8108	118
Qualcomm	msm8209	118
	msm8608	119
	msm8909w	120
	pm8937	120
	pmp8074	121
	qam8255p	121
	qam8295p	123
	qam8620p	124
	qam8650p	125
	qam8775p	126
	qamsrv1h	128
	qamsrv1m	129
	qca0000	130
	qca1062	131
	qca1064	131
	qca2062	132

Vendor	Product	Page Number
	qca2064	132
	qca2065	133
	qca2066	134
	qca4004	134
	qca4024	135
	qca6164	135
	qca6174	136
	qca6174a	136
	qca6310	137
	qca6320	138
	qca6335	139
	qca6391	139
	qca6420	142
	qca6421	143
	qca6426	144
Qualcomm	qca6428	146
Qualcomm	qca6430	147
	qca6431	148
	qca6436	149
	qca6438	151
	qca6554a	151
	qca6564	152
	qca6564a	153
	qca6564au	153
	qca6574	154
	qca6574a	155
	qca6574au	156
	qca6584au	158
	qca6595	159
	qca6595au	160
	qca6678aq	162
	qca6688aq	163

Vendor	Product	Page Number
	qca6694	164
	qca6696	164
	qca6698aq	166
	qca6777aq	167
	qca6787aq	168
	qca6797aq	169
	qca8072	170
	qca8075	170
	qca8081	171
	qca8082	172
	qca8084	172
	qca8085	172
	qca8337	173
	qca8386	174
	qca9377	175
Qualcomm	qca9379	175
Qualcomm	qcc2073	176
	qcc2076	177
	qcc710	178
	qcf8000	178
	qcf8001	179
	qcm2150	179
	qcm4325	179
	qcm5430	180
	qcm6490	180
	qcm8550	181
	qcn5124	182
	qcn6224	183
	qcn6274	183
	qcn6402	184
	qcn6412	185
	qcn6422	185

Vendor	Product	Page Number
	qcn6432	185
	qcn7605	186
	qcn7606	186
	qcn9000	186
	qcn9011	187
	qcn9012	187
	qcn9024	187
	qcn9074	188
	qcn9160	189
	qcn9274	189
	qcs2290	191
	qcs410	191
	qcs4290	193
	qcs4490	193
	qcs5430	193
Qualcomm	qcs610	194
Qualcomm	qcs6125	196
	qcs6490	196
	qcs7230	198
	qcs8155	199
	qcs8250	200
	qcs8550	201
	qcs9100	202
	qdu1000	203
	qdu1010	204
	qdu1110	204
	qdu1210	205
	qdx1010	206
	qdx1011	206
	qep8111	207
	qet4101	208
	qfw7114	208

Vendor	Product	Page Number
	qfw7124	209
	qrb5165m	210
	qrb5165n	211
	qru1032	211
	qru1052	212
	qru1062	213
	qsm8250	213
	qsm8350	215
	qsw8573	216
	qts110	216
	qxm8083	217
	robotics_rb3_platform	217
	robotics_rb5_platform	218
	sa2150p	218
	sa4150p	219
Qualcomm	sa4155p	219
Qualcomm	sa6145p	220
	sa6150p	222
	sa6155	223
	sa6155p	224
	sa7255p	226
	sa7775p	227
	sa8145p	228
	sa8150p	230
	sa8155	232
	sa8155p	232
	sa8195p	234
	sa8255p	236
	sa8295p	238
	sa8530p	240
	sa8540p	241
	sa8620p	243

Vendor	Product	Page Number
	sa8650p	244
	sa8770p	245
	sa8775p	247
	sa9000p	248
	sc8180x	250
	sc8380xp	251
	sd460	253
	sd660	253
	sd662	254
	sd670	254
	sd675	255
	sd730	256
	sd835	256
	sd855	257
	sd865_5g	257
Qualcomm	sd888	259
Qualcomm	sdm429w	260
	sdx20m	263
	sdx55	263
	sdx57m	265
	sdx61	266
	sdx65m	266
	sdx71m	267
	sd_455	267
	sd_675	268
	sd_8cx	268
	sd_8_gen1_5g	269
	sg4150p	270
	sg8275p	270
	sm4125	271
	sm4635	272
	sm6250	272

Vendor	Product	Page Number
	sm6250p	273
	sm6370	274
	sm7250p	274
	sm7315	275
	sm7325p	276
	sm8550p	276
	sm8635	278
	sm8750	279
	sm8750p	280
	smart_audio_200_platform	282
	smart_audio_400_platform	282
	snapdragon_1100_wearable_platform	283
	snapdragon_1200_wearable_platform	283
	snapdragon_208_processor	283
	snapdragon_210_processor	284
Qualcomm	snapdragon_212_mobile_platform	285
Qualcomm	snapdragon_425_mobile_platform	285
	snapdragon_427_mobile_platform	286
	snapdragon_429_mobile_platform	286
	snapdragon_430_mobile_platform	289
	snapdragon_435_mobile_platform	289
	snapdragon_439_mobile_platform	289
	snapdragon_460_mobile_platform	290
	<pre>snapdragon_480\+_5g_mobile_platform</pre>	290
	snapdragon_480_5g_mobile_platform	291
	snapdragon_4_gen_1_mobile_platform	292
	snapdragon_4_gen_2_mobile_platform	292
	snapdragon_630_mobile_platform	293
	snapdragon_636_mobile_platform	293
	snapdragon_660_mobile_platform	293
	snapdragon_662_mobile_platform	294
	snapdragon_665_mobile_platform	295

Vendor	Product	Page Number
	snapdragon_670_mobile_platform	295
	snapdragon_675_mobile_platform	296
	snapdragon_678_mobile_platform	296
	snapdragon_680_4g_mobile_platform	297
	snapdragon_685_4g_mobile_platform	298
	snapdragon_690_5g_mobile_platform	298
	snapdragon_695_5g_mobile_platform	299
	snapdragon_710_mobile_platform	300
	snapdragon_712_mobile_platform	300
	snapdragon_720g_mobile_platform	301
	snapdragon_730g_mobile_platform	301
	snapdragon_730_mobile_platform	302
	snapdragon_732g_mobile_platform	303
	snapdragon_750g_5g_mobile_platform	303
	snapdragon_765g_5g_mobile_platform	304
Qualcomm	snapdragon_765_5g_mobile_platform	305
Qualcomm	snapdragon_768g_5g_mobile_platform	306
	<pre>snapdragon_778g\+_5g_mobile_platform</pre>	307
	snapdragon_778g_5g_mobile_platform	308
	snapdragon_780g_5g_mobile_platform	309
	snapdragon_782g_mobile_platform	309
	<pre>snapdragon_7c\+_gen_3_compute</pre>	310
	snapdragon_7c_compute_platform	312
	snapdragon_7c_gen_2_compute_platform	312
	snapdragon_820_automotive_platform	313
	snapdragon_835_mobile_pc_platform	313
	snapdragon_845_mobile_platform	314
	snapdragon_850_mobile_compute_platform	314
	snapdragon_855\+	315
	snapdragon_855_mobile_platform	316
	snapdragon_860_mobile_platform	316
	snapdragon_865\+_5g_mobile_platform	317

Vendor	Product	Page Number
	snapdragon_865_5g_mobile_platform	319
	snapdragon_870_5g_mobile_platform	321
	snapdragon_888\+_5g_mobile_platform	324
	snapdragon_888_5g_mobile_platform	324
	snapdragon_8cx_compute_platform	325
	snapdragon_8cx_gen_2_5g_compute_platform	326
	snapdragon_8cx_gen_3_compute_platform	327
	snapdragon_8c_compute_platform	328
	snapdragon_8\+_gen_1_mobile_platform	329
	snapdragon_8\+_gen_2_mobile_platform	330
	snapdragon_8_gen_1_mobile_platform	331
	snapdragon_8_gen_2_mobile_platform	332
	snapdragon_8_gen_3_mobile_platform	333
	snapdragon_ar2_gen_1_platform	335
	snapdragon_auto_4g_modem	336
Qualcomm	snapdragon_auto_5g_modem-rf	337
Qualcomm	snapdragon_auto_5g_modem-rf_gen_2	337
	snapdragon_w5\+_gen_1_wearable_platform	338
	snapdragon_wear_1300_platform	340
	snapdragon_wear_2100_platform	340
	snapdragon_wear_2500_platform	341
	snapdragon_wear_3100_platform	341
	snapdragon_wear_4100\+_platform	342
	snapdragon_x12_lte_modem	343
	snapdragon_x20_lte_modem	343
	snapdragon_x24_lte_modem	343
	snapdragon_x35_5g_modem-rf_system	344
	snapdragon_x50_5g_modem-rf_system	345
	snapdragon_x55_5g_modem-rf_system	345
	snapdragon_x5_lte_modem	348
	snapdragon_x62_5g_modem-rf_system	348
	snapdragon_x65_5g_modem-rf_system	349

Vendor	Product	Page Number
	snapdragon_x70_modem-rf_system	350
	snapdragon_x72_5g_modem-rf_system	350
	snapdragon_x75_5g_modem-rf_system	351
	snapdragon_xr1_platform	352
	<pre>snapdragon_xr2\+_gen_1_platform</pre>	352
	snapdragon_xr2_5g_platform	353
	srv1h	355
	srv1l	357
	srv1m	357
	ssg2115p	359
	ssg2125p	360
	sw5100	361
	sw5100p	362
	sxr1120	364
	sxr1230p	364
Qualcomm	sxr2130	365
Qualcomm	sxr2230p	367
	sxr2250p	368
	talynplus	369
	video_collaboration_vc1_platform	369
	video_collaboration_vc3_platform	371
	video_collaboration_vc5_platform	373
	vision_intelligence_300_platform	374
	vision_intelligence_400_platform	375
	wcd9306	376
	wcd9326	377
	wcd9330	378
	wcd9335	378
	wcd9340	379
	wcd9341	381
	wcd9360	383
	wcd9370	384

Vendor	Product	Page Number
	wcd9371	387
	wcd9375	387
	wcd9378	389
	wcd9380	390
	wcd9385	393
	wcd9390	396
	wcd9395	397
	wcn3610	398
	wcn3615	398
	wcn3620	399
	wcn3660b	401
	wcn3680	405
	wcn3680b	405
	wcn3950	407
	wcn3980	408
Qualcomm	wcn3988	411
Qualcomm	wcn3990	413
	wcn3999	414
	wcn6740	415
	wcn6755	415
	wcn7860	417
	wcn7861	418
	wcn7880	419
	wcn7881	420
	wsa8810	422
	wsa8815	425
	wsa8830	427
	wsa8832	431
	wsa8835	433
	wsa8840	437
	wsa8845	439
	wsa8845h	442

Vendor	Product	Page Number
totolink	ex1800t	444
Tp-link	vn020_f3v	445
Operating System		
	ipados	446
	iphone_os	463
Annlo	macos	474
Apple	tvos	506
	visionos	516
	watchos	523
Huawei	harmonyos	533
Linux	linux_kernel	536
	windows	760
	windows_10_1507	761
	windows_10_1607	761
	windows_10_1809	761
	windows_10_21h2	761
	windows_10_22h2	762
	windows_11_22h2	762
Microsoft	windows_11_23h2	762
MICLOSOIL	windows_11_24h2	763
	windows_server_2008	763
	windows_server_2012	764
	windows_server_2016	764
	windows_server_2019	765
	windows_server_2022	765
	windows_server_2022_23h2	765
	windows_server_2025	766
openatom	openharmony	766
	205_mobile_platform_firmware	767
Qualcomm	215_mobile_platform_firmware	768
Qualcomm	315_5g_iot_modem_firmware	768
	9205_lte_modem_firmware	769

Vendor	Product	Page Number
	9206_lte_modem_firmware	769
	9207_lte_modem_firmware	769
	apq8017_firmware	770
	apq8037_firmware	770
	aqt1000_firmware	771
	ar8035_firmware	771
	c-v2x_9150_firmware	772
	csrb31024_firmware	773
	fastconnect_6200_firmware	773
	fastconnect_6700_firmware	775
	fastconnect_6800_firmware	776
	fastconnect_6900_firmware	779
	fastconnect_7800_firmware	783
	flight_rb5_5g_platform_firmware	786
	fsm10055_firmware	786
Qualcomm	fsm10056_firmware	787
Qualcomm	home_hub_100_platform_firmware	787
	immersive_home_214_platform_firmware	788
	immersive_home_216_platform_firmware	788
	immersive_home_316_platform_firmware	789
	immersive_home_318_platform_firmware	789
	immersive_home_3210_platform_firmware	789
	immersive_home_326_platform_firmware	790
	ipq5010_firmware	791
	ipq5028_firmware	791
	ipq5300_firmware	791
	ipq5302_firmware	792
	ipq5312_firmware	792
	ipq5332_firmware	793
	ipq6000_firmware	794
	ipq6005_firmware	794
	ipq6010_firmware	795

Vendor	Product	Page Number
	ipq6018_firmware	795
	ipq6028_firmware	795
	ipq8064_firmware	796
	ipq8065_firmware	796
	ipq8068_firmware	796
	ipq8070a_firmware	797
	ipq8070_firmware	797
	ipq8071a_firmware	797
	ipq8071_firmware	798
	ipq8072a_firmware	798
	ipq8072_firmware	799
	ipq8074a_firmware	799
	ipq8074_firmware	799
	ipq8076a_firmware	800
	ipq8076_firmware	800
Qualcomm	ipq8078a_firmware	800
Qualcollin	ipq8078_firmware	801
	ipq8173_firmware	801
	ipq8174_firmware	802
	ipq9008_firmware	802
	ipq9554_firmware	803
	ipq9570_firmware	803
	ipq9574_firmware	804
	mdm8207_firmware	805
	mdm9205s_firmware	805
	mdm9250_firmware	805
	mdm9628_firmware	806
	mdm9650_firmware	806
	msm8108_firmware	806
	msm8209_firmware	807
	msm8608_firmware	808
	msm8909w_firmware	808

Vendor	Product	Page Number
	pm8937_firmware	809
	pmp8074_firmware	809
	qam8255p_firmware	810
	qam8295p_firmware	811
	qam8620p_firmware	813
	qam8650p_firmware	814
	qam8775p_firmware	815
	qamsrv1h_firmware	816
	qamsrv1m_firmware	818
	qca0000_firmware	819
	qca1062_firmware	820
	qca1064_firmware	820
	qca2062_firmware	820
	qca2064_firmware	821
	qca2065_firmware	822
Qualcomm	qca2066_firmware	822
Qualcomm	qca4004_firmware	823
	qca4024_firmware	824
	qca6164_firmware	824
	qca6174a_firmware	824
	qca6174_firmware	826
	qca6310_firmware	826
	qca6320_firmware	827
	qca6335_firmware	827
	qca6391_firmware	828
	qca6420_firmware	831
	qca6421_firmware	832
	qca6426_firmware	833
	qca6428_firmware	835
	qca6430_firmware	835
	qca6431_firmware	836
	qca6436_firmware	837

Vendor	Product	Page Number
	qca6438_firmware	839
	qca6554a_firmware	840
	qca6564au_firmware	840
	qca6564a_firmware	841
	qca6564_firmware	842
	qca6574au_firmware	843
	qca6574a_firmware	845
	qca6574_firmware	846
	qca6584au_firmware	847
	qca6595au_firmware	848
	qca6595_firmware	849
	qca6678aq_firmware	850
	qca6688aq_firmware	852
	qca6694_firmware	852
	qca6696_firmware	853
Qualcomm	qca6698aq_firmware	855
Qualcomm	qca6777aq_firmware	856
	qca6787aq_firmware	856
	qca6797aq_firmware	857
	qca8072_firmware	858
	qca8075_firmware	858
	qca8081_firmware	859
	qca8082_firmware	860
	qca8084_firmware	860
	qca8085_firmware	861
	qca8337_firmware	861
	qca8386_firmware	863
	qca9377_firmware	863
	qca9379_firmware	864
	qcc2073_firmware	864
	qcc2076_firmware	865
	qcc710_firmware	866

Vendor	Product	Page Number
	qcf8000_firmware	867
	qcf8001_firmware	867
	qcm2150_firmware	868
	qcm4325_firmware	868
	qcm5430_firmware	868
	qcm6490_firmware	869
	qcm8550_firmware	870
	qcn5124_firmware	871
	qcn6224_firmware	871
	qcn6274_firmware	872
	qcn6402_firmware	873
	qcn6412_firmware	873
	qcn6422_firmware	873
	qcn6432_firmware	874
	qcn7605_firmware	874
Qualcomm	qcn7606_firmware	875
Qualcomm	qcn9000_firmware	875
	qcn9011_firmware	875
	qcn9012_firmware	876
	qcn9024_firmware	876
	qcn9074_firmware	876
	qcn9160_firmware	878
	qcn9274_firmware	878
	qcs2290_firmware	879
	qcs410_firmware	880
	qcs4290_firmware	881
	qcs4490_firmware	882
	qcs5430_firmware	882
	qcs610_firmware	883
	qcs6125_firmware	885
	qcs6490_firmware	885
	qcs7230_firmware	886

Vendor	Product	Page Number
	qcs8155_firmware	888
	qcs8250_firmware	888
	qcs8550_firmware	889
	qcs9100_firmware	891
	qdu1000_firmware	891
	qdu1010_firmware	892
	qdu1110_firmware	893
	qdu1210_firmware	893
	qdx1010_firmware	894
	qdx1011_firmware	895
	qep8111_firmware	895
	qet4101_firmware	896
	qfw7114_firmware	897
	qfw7124_firmware	897
	qrb5165m_firmware	898
Qualcomm	qrb5165n_firmware	899
Qualcomm	qru1032_firmware	900
	qru1052_firmware	900
	qru1062_firmware	901
	qsm8250_firmware	902
	qsm8350_firmware	904
	qsw8573_firmware	904
	qts110_firmware	905
	qxm8083_firmware	905
	robotics_rb3_platform_firmware	906
	robotics_rb5_platform_firmware	906
	sa2150p_firmware	907
	sa4150p_firmware	907
	sa4155p_firmware	908
	sa6145p_firmware	909
	sa6150p_firmware	910
	sa6155p_firmware	912

Vendor	Product	Page Number
	sa6155_firmware	914
	sa7255p_firmware	914
	sa7775p_firmware	916
	sa8145p_firmware	917
	sa8150p_firmware	919
	sa8155p_firmware	920
	sa8155_firmware	922
	sa8195p_firmware	923
	sa8255p_firmware	925
	sa8295p_firmware	926
	sa8530p_firmware	928
	sa8540p_firmware	930
	sa8620p_firmware	931
	sa8650p_firmware	933
	sa8770p_firmware	934
Qualaamm	sa8775p_firmware	935
Qualcomm	sa9000p_firmware	937
	sc8180x_firmware	939
	sc8380xp_firmware	940
	sd460_firmware	942
	sd660_firmware	942
	sd662_firmware	942
	sd670_firmware	943
	sd675_firmware	943
	sd730_firmware	944
	sd835_firmware	945
	sd855_firmware	945
	sd865_5g_firmware	946
	sd888_firmware	948
	sdm429w_firmware	949
	sdx20m_firmware	951
	sdx55_firmware	952

Vendor	Product	Page Number
	sdx57m_firmware	954
	sdx61_firmware	955
	sdx65m_firmware	955
	sdx71m_firmware	956
	sd_455_firmware	956
	sd_675_firmware	956
	sd_8cx_firmware	957
	sd_8_gen1_5g_firmware	958
	sg4150p_firmware	958
	sg8275p_firmware	959
	sm4125_firmware	960
	sm4635_firmware	960
	sm6250p_firmware	961
	sm6250_firmware	962
	sm6370_firmware	962
	sm7250p_firmware	963
Qualcomm	sm7315_firmware	964
	sm7325p_firmware	964
	sm8550p_firmware	965
	sm8635_firmware	966
	sm8750p_firmware	968
	sm8750_firmware	969
	smart_audio_200_platform_firmware	970
	smart_audio_400_platform_firmware	971
	snapdragon_1100_wearable_platform_firmwa re	971
	snapdragon_1200_wearable_platform_firmwa re	972
	snapdragon_208_processor_firmware	972
	snapdragon_210_processor_firmware	973
	snapdragon_212_mobile_platform_firmware	973
	snapdragon_425_mobile_platform_firmware	974
	snapdragon_427_mobile_platform_firmware	974

Vendor	Product	Page Number
	snapdragon_429_mobile_platform_firmware	975
	snapdragon_430_mobile_platform_firmware	977
	snapdragon_435_mobile_platform_firmware	978
	snapdragon_439_mobile_platform_firmware	978
	snapdragon_460_mobile_platform_firmware	978
	snapdragon_480\+_5g_mobile_platform_firm ware	979
	snapdragon_480_5g_mobile_platform_firmwar e	980
	snapdragon_4_gen_1_mobile_platform_firmwa re	980
	snapdragon_4_gen_2_mobile_platform_firmwa re	981
	snapdragon_630_mobile_platform_firmware	982
	snapdragon_636_mobile_platform_firmware	982
	snapdragon_660_mobile_platform_firmware	982
Qualcomm	snapdragon_662_mobile_platform_firmware	983
Qualcomm	snapdragon_665_mobile_platform_firmware	983
	snapdragon_670_mobile_platform_firmware	984
	snapdragon_675_mobile_platform_firmware	984
	snapdragon_678_mobile_platform_firmware	985
	snapdragon_680_4g_mobile_platform_firmwar e	986
e snapdragon e	snapdragon_685_4g_mobile_platform_firmwar e	986
	snapdragon_690_5g_mobile_platform_firmwar e	987
	snapdragon_695_5g_mobile_platform_firmwar e	988
	snapdragon_710_mobile_platform_firmware	989
	snapdragon_712_mobile_platform_firmware	989
	snapdragon_720g_mobile_platform_firmware	989
	snapdragon_730g_mobile_platform_firmware	990
	snapdragon_730_mobile_platform_firmware	991

Vendor	Product	Page Number
	snapdragon_732g_mobile_platform_firmware	991
	snapdragon_750g_5g_mobile_platform_firmwa re	992
	snapdragon_765g_5g_mobile_platform_firmwa re	993
	snapdragon_765_5g_mobile_platform_firmwar e	994
	snapdragon_768g_5g_mobile_platform_firmwa re	995
	snapdragon_778g\+_5g_mobile_platform_firm ware	996
	snapdragon_778g_5g_mobile_platform_firmwa re	997
	snapdragon_780g_5g_mobile_platform_firmwa re	997
	snapdragon_782g_mobile_platform_firmware	998
	snapdragon_7c\+_gen_3_compute_firmware	999
Qualcomm	snapdragon_7c_compute_platform_firmware	1000
Qualcomin	snapdragon_7c_gen_2_compute_platform_firm ware	1001
	snapdragon_820_automotive_platform_firmwa re	1002
	snapdragon_835_mobile_pc_platform_firmwar e	1002
	snapdragon_845_mobile_platform_firmware	1003
	snapdragon_850_mobile_compute_platform_fi rmware	1003
	snapdragon_855\+_firmware	1004
	snapdragon_855_mobile_platform_firmware	1005
	snapdragon_860_mobile_platform_firmware	1005
	snapdragon_865\+_5g_mobile_platform_firm ware	1006
	snapdragon_865_5g_mobile_platform_firmwar e	1008
	snapdragon_870_5g_mobile_platform_firmwar e	1010

Vendor	Product	Page Number
	snapdragon_888\+_5g_mobile_platform_firm ware	1013
	snapdragon_888_5g_mobile_platform_firmwar e	1013
	snapdragon_8cx_compute_platform_firmware	1014
	snapdragon_8cx_gen_2_5g_compute_platform_ firmware	1015
	snapdragon_8cx_gen_3_compute_platform_fir mware	1016
	snapdragon_8c_compute_platform_firmware	1017
	snapdragon_8\+_gen_1_mobile_platform_firm ware	1018
	snapdragon_8\+_gen_2_mobile_platform_firm ware	1019
	snapdragon_8_gen_1_mobile_platform_firmwa re	1020
	snapdragon_8_gen_2_mobile_platform_firmwa re	1021
Qualcomm	snapdragon_8_gen_3_mobile_platform_firmwa re	1022
	snapdragon_ar2_gen_1_platform_firmware	1024
	snapdragon_auto_4g_modem_firmware	1025
	snapdragon_auto_5g_modem-rf_firmware	1026
	snapdragon_auto_5g_modem- rf_gen_2_firmware	1026
	snapdragon_w5\+_gen_1_wearable_platform_f irmware	1027
	snapdragon_wear_1300_platform_firmware	1029
	snapdragon_wear_2100_platform_firmware	1029
	snapdragon_wear_2500_platform_firmware	1030
	snapdragon_wear_3100_platform_firmware	1030
	snapdragon_wear_4100\+_platform_firmware	1031
	snapdragon_x12_lte_modem_firmware	1032
	snapdragon_x20_lte_modem_firmware	1032
	snapdragon_x24_lte_modem_firmware	1032

Vendor	Product	Page Number
	snapdragon_x35_5g_modem- rf_system_firmware	1033
	snapdragon_x50_5g_modem- rf_system_firmware	1034
	snapdragon_x55_5g_modem- rf_system_firmware	1034
	snapdragon_x5_lte_modem_firmware	1037
	snapdragon_x62_5g_modem- rf_system_firmware	1037
	snapdragon_x65_5g_modem- rf_system_firmware	1038
	snapdragon_x70_modem-rf_system_firmware	1039
	snapdragon_x72_5g_modem- rf_system_firmware	1039
	snapdragon_x75_5g_modem- rf_system_firmware	1040
	snapdragon_xr1_platform_firmware	1041
Qualcomm	snapdragon_xr2\+_gen_1_platform_firmware	1041
Qualcomm	snapdragon_xr2_5g_platform_firmware	1042
	srv1h_firmware	1044
	srv1l_firmware	1046
	srv1m_firmware	1046
	ssg2115p_firmware	1048
	ssg2125p_firmware	1049
	sw5100p_firmware	1050
	sw5100_firmware	1051
	sxr1120_firmware	1053
	sxr1230p_firmware	1053
	sxr2130_firmware	1054
	sxr2230p_firmware	1056
	sxr2250p_firmware	1057
	talynplus_firmware	1058
	video_collaboration_vc1_platform_firmware	1058
	video_collaboration_vc3_platform_firmware	1060

Vendor	Product	Page Number
	video_collaboration_vc5_platform_firmware	1062
	vision_intelligence_300_platform_firmware	1063
	vision_intelligence_400_platform_firmware	1064
	wcd9306_firmware	1065
	wcd9326_firmware	1066
	wcd9330_firmware	1067
	wcd9335_firmware	1067
	wcd9340_firmware	1068
	wcd9341_firmware	1070
	wcd9360_firmware	1072
	wcd9370_firmware	1073
	wcd9371_firmware	1076
	wcd9375_firmware	1076
	wcd9378_firmware	1078
	wcd9380_firmware	1079
Qualcomm	wcd9385_firmware	1082
Qualcomm	wcd9390_firmware	1085
	wcd9395_firmware	1086
	wcn3610_firmware	1087
	wcn3615_firmware	1087
	wcn3620_firmware	1088
	wcn3660b_firmware	1090
	wcn3680b_firmware	1093
	wcn3680_firmware	1095
	wcn3950_firmware	1096
	wcn3980_firmware	1097
	wcn3988_firmware	1099
	wcn3990_firmware	1102
	wcn3999_firmware	1103
	wcn6740_firmware	1104
	wcn6755_firmware	1104
	wcn7860_firmware	1106

Vendor	Product	Page Number
	wcn7861_firmware	1107
	wcn7880_firmware	1108
	wcn7881_firmware	1109
	wsa8810_firmware	1111
	wsa8815_firmware	1114
Qualcomm	wsa8830_firmware	1116
	wsa8832_firmware	1120
	wsa8835_firmware	1122
	wsa8840_firmware	1126
	wsa8845h_firmware	1128
	wsa8845_firmware	1131
ruijienetworks	reyee_os	1133
totolink	ex1800t_firmware	1136
Tp-link	vn020_f3v_firmware	1136

Common Vulnerabilities and Exposures (CVE) Report						
Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
	1		Application			
Vendor: 10	00projects					
Product: at	tendance_track	king_man	agement_system			
Affected Ver	sion(s): 1.0					
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	12-Dec-2024	7.3	A vulnerability classified as critical has been found in 1000 Projects Attendance Tracking Management System 1.0. Affected is an unknown function of the file /admin/check_admin_login. php. The manipulation of the argument admin_user_name leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12497	N/A	A-100-ATTE- 201224/1	
Product: be	auty_parlour_i	nanagem	ent_system	1		
Affected Ver	sion(s): 1.0					
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	05-Dec-2024	7.3	A vulnerability was found in 1000 Projects Beauty Parlour Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/edit-customer- detailed.php. The manipulation of the argument name leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other	N/A	A-100-BEAU- 201224/2	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameters might be affected as well.		
			CVE ID : CVE-2024-12234		
Product: lib	rary_managen	nent_syst	em		
Affected Vers	sion(s): 1.0				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	05-Dec-2024	7.3	A vulnerability was found in 1000 Projects Library Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /showbook.php. The manipulation of the argument q 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-2024-12187	N/A	A-100-LIBR- 201224/3
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	05-Dec-2024	7.3	A vulnerability was found in 1000 Projects Library Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /brains/stu.php. The manipulation of the argument useri 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-2024-12188	N/A	A-100-LIBR- 201224/4
Vendor: Adobe					
Product: bridge					
Affected Ver	sion(s): * Up to	(excluding	g) 14.1.4		
Affected Version(s): * Up to (excluding) 14.1.4					

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparoun d)	10-Dec-2024	7.8	Bridge versions 14.1.3, 15.0 and earlier are affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2024-53955	https:// helpx.ad obe.com /securit y/produ cts/brid ge/apsb 24- 103.htm l	A-ADO-BRID- 201224/5
Affected Ver	sion(s): 15.0				
Integer Underflow (Wrap or Wraparoun d)	10-Dec-2024	7.8	Bridge versions 14.1.3, 15.0 and earlier are affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2024-53955	https:// helpx.ad obe.com /securit y/produ cts/brid ge/apsb 24- 103.htm l	A-ADO-BRID- 201224/6
Product: ex	perience_mana	ager		·	
Affected Ver	sion(s): * Up to	(excluding			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/7

9-10

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		to the page containing the vulnerable field.		
		CVE ID : CVE-2024-52827		
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/8
		CVE ID : CVE-2024-52828		
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52829	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/9
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/10
	 10-Dec-2024 10-Dec-2024	и и	10-Dec-20245.4to the page containing the vulnerable field. CVE ID : CVE-2024-5282710-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-5282810-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerability that could be abused by an attacker to inject malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-5282910-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerabile field. CVE ID : CVE-2024-5282910-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerabile field. CVE ID : CVE-2024-52829	10-Dec-20245.4to the page containing the vulnerable field. CVE ID : CVE-2024-5282710-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-5282810-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious savaScript may be executed in a victim's browser when they browse to the page containing the vulnerability that could be abused by an attacker to inject malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-5282910-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52829https:// helpx.ad obe.com /securit yprodu cts/expe rience- manager10-Dec-20245.4Adobe Experience Manager vulnerable form fields. Malicious JavaScript may be executed in a victim's belex.ad obe.com /securit vulnerable form fields. Malicious JavaScript may be executed in a victim's /securit vulnerable form fields. Malicious JavaScript may be

		Description & CVE ID	Patch	NCIIPC ID
		to the page containing the vulnerable field.		
		CVE ID : CVE-2024-52830		
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/11
		CVE ID : CVE-2024-53960		
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52832	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/12
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/13
	10-Dec-2024	10-Dec-2024 5.4	10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by	10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerable field.https:// helpx.ad obe.com10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be execurted in a victim's

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		to the page containing the vulnerable field.		
		CVE ID : CVE-2024-52834		
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/14
		CVE ID : CVE-2024-52835		
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52836	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/15
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/16
	10-Dec-2024	 Normal (1) Normal (1)	10-Dec-20245.4to the page containing the vulnerable field. CVE ID : CVE-2024-5283410-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-5283510-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerability that could be abused by an attacker to inject malicious script may be executed in a victim's browser when they browse to the page containing the vulnerability that could be abused by an attacker to inject malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious script may be executed in a victim's browser when they browse to the page containing the vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerability that could be abused by an attacker to inject malicious scripts into vulnerability that could be abused by an attacker to inject malicious s	10-Dec-20245.4to the page containing the vulnerable field.Inttps:// helpx.ad obe.com10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields.https:// helpx.ad obe.com10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored niject malicious scripts into vulnerable form fields.https:// helpx.ad obe.com10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerable field.https:// helpx.ad obe.com10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored inject malicious scripts into

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		to the page containing the vulnerable field.		
		CVE ID : CVE-2024-52841		
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/17
		CVE ID : CVE-2024-52842		
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52843	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/18
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/19
	10-Dec-2024	а с с с с с с с с с с с с с с с с с с с	10-Dec-20245.4to the page containing the vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerable form fields. Malicious JavaScript into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.10-Dec-20	10-Dec-20245.4to the page containing the vulnerable field.io the page containing the vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored oble.com abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.https:// helpx.ad oble.com /securit y/produ cts/expe rience- manager /apsb24 -69.html10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored cross-Site Scripting (XSS) vulnerable field.https:// helpx.ad oble.com /securit y/produ cts/expe rience- manager

	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		to the page containing the vulnerable field.		
		CVE ID : CVE-2024-52845		
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/20
		CVE ID : CVE-2024-52846		
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52847	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/21
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/22
	10-Dec-2024	10-Dec-2024 5.4	10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and actime they browse to the page containing the vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicous scripts into	10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerabile field.https:// helpx.ad obe.com10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's

		to the page containing the vulnerable field.		
		CVE ID : CVE-2024-52848		
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/23
		CVE ID : CVE-2024-52849		
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52850	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/24
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/25
	10-Dec-2024	10-Dec-2024 5.4 10-Dec-2024 5.4	Image: constraint of the second sec	Image: 10-Dec-2024CVE ID : CVE-2024-52848Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerabile field.https:// helpx.ad obe.com10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable field.https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored cross-Site Scripting (XSS) vulnerable field.https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager10-Dec-20245.4Adobe Experience Manager vulnerable field.https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html10-Dec-20245.4Adobe Experience Manager vulnerable field.https:// helpx.ad obe.com /securit y/produ cts/expe /securit vulnerable field.10-

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		to the page containing the vulnerable field.		
		CVE ID : CVE-2024-52851		
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/26
		CVE ID : CVE-2024-52852		
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52853	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/27
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/28
	 10-Dec-2024 10-Dec-2024	и и	10-Dec-20245.4to the page containing the vulnerable field. CVE ID : CVE-2024-5285110-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-5285210-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerability that could be abused by an attacker to inject malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-5285310-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerabile field. CVE ID : CVE-2024-5285310-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerabile field. CVE ID : CVE-2024-52853	10-Dec-20245.4to the page containing the vulnerable field. CVE ID : CVE-2024-5285110-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52852https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerable form fields. Malicious JavaScript may be abused by an attacker to inject malicious scripts into vulnerability that could be abused by an attacker to inject malicious scripts into vulne

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		to the page containing the vulnerable field.		
		CVE ID : CVE-2024-52854		
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/29
		CVE ID : CVE-2024-52855		
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52857	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/30
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/31
	 10-Dec-2024 10-Dec-2024	и и	10-Dec-20245.4to the page containing the vulnerable field. CVE ID : CVE-2024-5285410-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-5285510-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerability that could be abused by an attacker to inject malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-5285710-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerabile field. CVE ID : CVE-2024-5285710-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerabile field. CVE ID : CVE-2024-52857	10-Dec-20245.4to the page containing the vulnerable field.to the page containing the vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored (Cross-Site Scripting (XSS) vulnerablity that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious savaScript may be executed in a victim's browser when they browse to the page containing the vulnerability that could be abused by an attacker to inject malicious savaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerable field.https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager10-Dec-20245.4Adobe Experience Manager vulnerable field.https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html10-Dec-20245.4Adobe Experience Manager

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field.		
			CVE ID : CVE-2024-52858		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/32
			CVE ID : CVE-2024-52859		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability that could be exploited by an attacker to execute arbitrary code in the context of the victim's browser session. By manipulating a DOM element through a crafted URL or user input, the attacker can inject malicious scripts that run when the page is rendered. User interaction is required for exploitation, as a victim must visit a malicious link or input data into a vulnerable web application. CVE ID : CVE-2024-52860	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/33
Improper			Adobe Experience Manager	https://	A-ADO-EXPE-
Neutralizat ion of	10-Dec-2024	5.4	versions 6.5.21 and earlier are affected by a stored	helpx.ad obe.com	201224/34
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
Input During Web Page Generation ('Cross-site Scripting')			Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	/securit y/produ cts/expe rience- manager /apsb24 -69.html	
			CVE ID : CVE-2024-52861		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/35
			CVE ID : CVE-2024-52862		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/36
T			CVE ID : CVE-2024-52864	1	
Improper Neutralizat ion of	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored	https:// helpx.ad obe.com	A-ADO-EXPE- 201224/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	/securit y/produ cts/expe rience- manager /apsb24 -69.html	
			CVE ID : CVE-2024-52991		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52992	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/38
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52993	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/39
Improper Neutralizat ion of	10-Dec-2024	4.6	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored	https:// helpx.ad obe.com	A-ADO-EXPE- 201224/40

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Cross-Site Scripting (XSS) vulnerability that could be abused by a privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52865	/securit y/produ cts/expe rience- manager /apsb24 -69.html	
Improper Input Validation	10-Dec-2024	3.5	Adobe Experience Manager versions 6.5.21 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/41
			CVE ID : CVE-2024-52831		
Affected Ver	sion(s): * Up to	(excluding		T	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52827	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/43
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	CVE ID : CVE-2024-52828 Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52829	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/44
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52830	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/45

Improper Neutralization of Improper Cross-site Scripting')10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable field.https:// helpx.ad obe.com /securit 4-69.htmlImproper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored cross-Site Scripting (XSS) vulnerable field.https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /securit y/produ cts/expe /apsb24Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored cross-Site Scripting (XSS) vulnerable field.https:// helpx.ad obe.com /securit y/produ cts/expe fience- manager /apsb24Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored cross-Site Scripting (XSS) vulnerable field.https:// Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored vulnerable field.Improper Neutralizat ion of Inp	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During ('Cross-site Scripting')10-Dec-2024Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored abused by an attacker to inject malicious scripts into vulnerability that could be abused by an attacker to unerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.A-ADO-EXPE- 201224/47Improper Neutralizat ion of ('Cross-site Scripting')10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to vulnerable field.A-ADO-EXPE- 201224/47Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into yulnerability that could be abused by an attacker to inject malicious scripts into yprodu cts/expe rence- manager / A-ADO-EXPE- 201224/48Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')5.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Adobe Experience Manager versions 6.5.21 and earlier are affected by a attacker to inject malicious scripts into yprodu cts/expe rence- manager / helpx.ad obe.comImproper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') </td <td>Neutralizat ion of Input During Web Page Generation ('Cross-site</td> <td>10-Dec-2024</td> <td>5.4</td> <td>versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the</td> <td>helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24</td> <td></td>	Neutralizat ion of Input During Web Page Generation ('Cross-site	10-Dec-2024	5.4	versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the	helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')10-Dec-20245.4are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.htmlA-ADO-EXPE- 201224/47Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerability that could be abused by an attacker to inject malicious scripts into vulnerability that could be abused by an attacker to inject malicious scripts into vulnerability that could be abused by an attacker to inject malicious scripts into vulnerability that could be abused by an attacker to inject malicious scripts into vulnerability that could be abused by an attacker to inject malicious scripts into vulnerabile form fields.A-ADO-EXPE- 201224/48Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')5.4Adobe Experime Page excuted in a victim's browser when they browse 				Adobe Experience Manager		
Improper Neutralizat ion of Input During10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored vulnerability that could be abused by an attacker to vulnerable form fields.https:// helpx.ad obe.com /securit y/produA-ADO-EXPE- 201224/48Web Page Generation ('Cross-site Scripting')10-Dec-20245.46.46.51.4Malicious JavaScript may be browser when they browse to the page containing therience- manager -69.html1.41.4	Neutralizat ion of Input During Web Page Generation ('Cross-site	10-Dec-2024	5.4	are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the	helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24	
Improper Neutralizat ion of Input During10-Dec-20245.4versions 6.5.21 and earlier are affected by a stored Unerability that could be abused by an attacker to vulnerability that could be abused by an attacker to vulnerable form fields.https:// helpx.ad obe.com /securit y/produ cts/expe 201224/48Web Page Generation ('Cross-site Scripting')10-Dec-20245.4A-ADO-EXPE- 201224/48				CVE ID : CVE-2024-52832		
vulnerable field. CVE ID : CVE-2024-52834	Neutralizat ion of Input During Web Page Generation ('Cross-site	10-Dec-2024	5.4	versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/49
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	CVE ID : CVE-2024-52835 Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52836	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/50
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52841	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/51

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/52
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	CVE ID : CVE-2024-52842 Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52843	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/53
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52845	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/55
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	CVE ID : CVE-2024-52846 Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52847	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/56
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52848	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/58
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	CVE ID : CVE-2024-52849 Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52850	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/59
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52851	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/61
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	CVE ID : CVE-2024-52852 Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52853	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/62
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52854	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/64
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	CVE ID : CVE-2024-52855 Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52857	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/65
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52858	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/66

				NCIIPC ID
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/67
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability that could be exploited by an attacker to execute arbitrary code in the context of the victim's browser session. By manipulating a DOM element through a crafted URL or user input, the attacker can inject malicious scripts that run when the page is rendered. User interaction is required for exploitation, as a victim must visit a malicious link or input data into a vulnerable web application. CVE ID : CVE-2024-52860	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/68
10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into	https:// helpx.ad obe.com /securit y/produ cts/expe rience-	A-ADO-EXPE- 201224/69
	10-Dec-2024	10-Dec-2024 5.4	10-Dec-20245.4versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability that could be exploited by an attacker to execute arbitrary code in the context of the victim's browser session. By manipulating a DOM element through a crafted URL or user input, the attacker can inject malicious scripts that run when the page is rendered. User interaction is required for exploitation, as a victim must visit a malicious link or input data into a vulnerable web application. CVE ID : CVE-2024-5286010-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be avantacker to a vulnerable web application. CVE ID : CVE-2024-52860	10-Dec-20245.4versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52859https:// helpx.ad obe.com /securit /apsb24 -69.html10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability that could be exploited by an attacker to execute arbitrary code in the context of the victim's browser session. By manipulating a DOM element through a crafted URL or user input, the attacker can inject malicious scripts that run when the page is rendered. User interaction is required for exploitation, as a victim must visit a malicious link or input data into a vulnerable web application. CVE ID : CVE-2024-52860https:// helpx.ad obe.com10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored or exploitation, as a victim must visit a malicious link or input data into a vulnerable web application. CVE ID : CVE-2024-52860https:// helpx.ad obe.com10-Dec-20245.4Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored obe.comhttps:// helpx.ad obe.com10-Dec-20245.4Adobe Experience Manager vulnerability that could be a stored cross-Site Scripting (XSS) vulnerability that could be a stored cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to cross-site Scri

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	manager /apsb24 -69.html	
			CVE ID : CVE-2024-52861		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52862	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/70
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52864	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/71
Improper Neutralizat ion of Input During Web Page Generation	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into	https:// helpx.ad obe.com /securit y/produ cts/expe rience-	A-ADO-EXPE- 201224/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	manager /apsb24 -69.html	
			CVE ID : CVE-2024-52991		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52992	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/73
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2024-52993	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/74
Improper Neutralizat ion of Input During Web Page Generation	10-Dec-2024	4.6	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a privileged attacker to inject malicious	https:// helpx.ad obe.com /securit y/produ cts/expe rience-	A-ADO-EXPE- 201224/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	manager /apsb24 -69.html	
			CVE ID : CVE-2024-52865		
Improper Input Validation	10-Dec-2024	3.5	Adobe Experience Manager versions 6.5.21 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https:// helpx.ad obe.com /securit y/produ cts/expe rience- manager /apsb24 -69.html	A-ADO-EXPE- 201224/76
			CVE ID : CVE-2024-52831		
Product: fra					
Affected Ver	sion(s): * Up to	(excluding			
Stack- based Buffer Overflow	10-Dec-2024	7.8	Adobe Framemaker versions 2020.7, 2022.5 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https:// helpx.ad obe.com /securit y/produ cts/fram emaker/ apsb24- 106.htm l	A-ADO-FRAM- 201224/77
			CVE ID : CVE-2024-53959		
Affected Ver	sion(s): From (i	ncluding)	2022 Up to (excluding) 2022.5	1	
Stack- based	10-Dec-2024	7.8	Adobe Framemaker versions 2020.7, 2022.5 and earlier are affected by a Stack-based Buffer	https:// helpx.ad obe.com /securit	A-ADO-FRAM- 201224/78

Weakness	Publish Date	CVSSv3	Descr	iption & (CVE ID		Patch	NCII	PC ID
Buffer Overflow			Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2024-53959			ct: en ap 10	'produ s/fram naker/ osb24-)6.htm		
Product: pro	emiere_pro								
		(excludin	g) 24.6.4						
Affected Version(s): * Up to (excluding) 24.6.4Affected Version(s): * Up to (excluding) 24.6.4Premiere Pro versions 25.0, 24.6.3 and earlier are affected by a Heap-based Buffer Overflow10-Dec-20247.87.8Premiere Pro versions 25.0, 24.6.3 and earlier are affected by a Heap-based vulnerability that could result in arbitrary code execution in the context of the current user.0verflow10-Dec-20247.8610-Dec-20247.87.97.97.97.97.97									
Affected Ver	sion(s): 25.0								
Heap- based Buffer Overflow	10-Dec-2024	7.8	Premiere 24.6.3 and affected b Buffer Ove vulnerabi result in a execution the curren Exploitati requires u that a vict malicious CVE ID : C	l earlier y a Heap erflow lity that rbitrary in the co nt user. on of thi iser inter im must file.	are -based could code ontext of s issue caction in open a	htt he ob /s y/ ct: m ro 24 10	tps:// elpx.ad be.com ecurit /produ s/pre iere_p /apsb I-)4.htm	A-ADO- 201224	
Product: su	bstance_3d_mo	odeler	l						
Affected Ver	sion(s): * Up to	(including	g) 1.14.1						
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
Heap- based Buffer Overflow	10-Dec-2024	7.8	Substance3D - Modeler versions 1.14.1 and earlier are affected by a Heap- based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2024-52999	https:// helpx.ad obe.com /securit y/produ cts/subs tance3d- modeler /apsb24 - 102.htm l	A-ADO-SUBS- 201224/81
Out-of- bounds Write	10-Dec-2024	7.8	Substance3D - Modeler versions 1.14.1 and earlier are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2024-53000	https:// helpx.ad obe.com /securit y/produ cts/subs tance3d- modeler /apsb24 - 102.htm l	A-ADO-SUBS- 201224/82
Out-of- bounds Write	10-Dec-2024	7.8	Substance3D - Modeler versions 1.14.1 and earlier are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2024-53001	https:// helpx.ad obe.com /securit y/produ cts/subs tance3d- modeler /apsb24 - 102.htm l	A-ADO-SUBS- 201224/83
Out-of- bounds Write	10-Dec-2024	7.8	Substance3D - Modeler versions 1.14.1 and earlier are affected by an out-of- bounds write vulnerability that could result in	https:// helpx.ad obe.com /securit y/produ	A-ADO-SUBS- 201224/84
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
			arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	cts/subs tance3d- modeler /apsb24 - 102.htm	
			CVE ID : CVE-2024-53002	1	
Out-of- bounds Write	10-Dec-2024	7.8	Substance3D - Modeler versions 1.14.1 and earlier are affected by an out-of- bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https:// helpx.ad obe.com /securit y/produ cts/subs tance3d- modeler /apsb24 - 102.htm	A-ADO-SUBS- 201224/85
			CVE ID : CVE-2024-53003	1	
Out-of- bounds Read	10-Dec-2024	5.5	Substance3D - Modeler versions 1.14.1 and earlier are affected by an out-of- bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2024-53004	https:// helpx.ad obe.com /securit y/produ cts/subs tance3d- modeler /apsb24 - 102.htm l	A-ADO-SUBS- 201224/86
Out-of- bounds Read	10-Dec-2024	5.5	Substance3D - Modeler versions 1.14.1 and earlier are affected by an out-of- bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR.	https:// helpx.ad obe.com /securit y/produ cts/subs tance3d- modeler /apsb24	A-ADO-SUBS- 201224/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file.	- 102.htm 1	
			CVE ID : CVE-2024-53005		
NULL Pointer Dereferenc e	10-Dec-2024	5.5	Substance3D - Modeler versions 1.14.1 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https:// helpx.ad obe.com /securit y/produ cts/subs tance3d- modeler /apsb24 - 102.htm l	A-ADO-SUBS- 201224/88
D			CVE ID : CVE-2024-53006		
	bstance_3d_pa		-) 10 1 2		
Affected ver	sion(s): * Up to	(excluding			
Heap- based Buffer Overflow	10-Dec-2024	7.8	Substance3D - Painter versions 10.1.1 and earlier are affected by a Heap- based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2024-53957	https:// helpx.ad obe.com /securit y/produ cts/subs tance3d_ painter/ apsb24- 105.htm l	A-ADO-SUBS- 201224/89
				h	
Out-of- bounds Write	10-Dec-2024	7.8	Substance3D - Painter versions 10.1.1 and earlier are affected by an out-of- bounds write vulnerability that could result in	https:// helpx.ad obe.com /securit y/produ	A-ADO-SUBS- 201224/90

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2024-53958	cts/subs tance3d_ painter/ apsb24- 105.htm l	
Vendor: ani	sha				
Product: far	macia				
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection'	12-Dec-2024	6.3	A vulnerability was found in code-projects Farmacia 1.0. It has been rated as critical. This issue affects some unknown processing of the file /visualizar-usuario.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	N/A	A-ANI-FARM- 201224/91
J			CVE ID : CVE-2024-12492		
Vendor: anı	ıjk305				
Product: me	edical_card_gei	neration_	system		
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2024	4.8	PhpGurukul Medical Card Generation System v1.0 is vulnerable to Cross Site Scripting (XSS) in /admin/search- medicalcard.php via the searchdata parameter. CVE ID : CVE-2024-48703	N/A	A-ANU-MEDI- 201224/92
Vendor: App	ple				
Product: saf	fari				
Affected Ver	sion(s): * Up to	(excluding	g) 18.1		
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Origin Validation Error	12-Dec-2024	5.3	A cookie management issue was addressed with improved state management. This issue is fixed in Safari 18.1, visionOS 2.1, tvOS 18.1, iOS 18.1 and iPadOS 18.1, watchOS 11.1. Cookies belonging to one origin may be sent to another origin. CVE ID : CVE-2024-44212	https:// support. apple.co m/en- us/1215 63, https:// support. apple.co m/en- us/1215 65, https:// support. apple.co m/en- us/1215 66, https:// support. apple.co m/en- us/1215 66, https:// support. apple.co m/en- us/1215 71	A-APP-SAFA- 201224/93
Affected Ver	sion(s): * Up to	(excluding	g) 18.2		
Out-of- bounds Write	12-Dec-2024	9.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS		A-APP-SAFA- 201224/94

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
				https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 45, https:// support. apple.co m/en- us/1218 45,	
Access of Resource Using Incompatib le Type ('Type Confusion')	12-Dec-2024	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. CVE ID : CVE-2024-54505	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support.	A-APP-SAFA- 201224/95

				apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 45	
N/A	12-Dec-2024	7.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. CVE ID : CVE-2024-54479	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en-	A-APP-SAFA- 201224/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/1218 44, https:// support. apple.co m/en- us/1218 45 https:// support.	
N/A	12-Dec-2024	7.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. CVE ID : CVE-2024-54508	apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 45, https:// support. apple.co m/en- us/1218	A-APP-SAFA- 201224/97

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					
				us/1218 46						
Vendor: cjb	i									
Product: we	Product: wetech-cms									
Affected Ver	sion(s): 1.0									
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	12-Dec-2024	6.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2 and classified as critical. This issue affects the function searchTopicByKeyword of the file wetech-cms- master\wetech- core\src\main\java\tech\ wetech\cms\dao\TopicDao .java. The manipulation of the argument keyword leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. CVE ID : CVE-2024-12479	N/A	A-CJB-WETE- 201224/98					
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	12-Dec-2024	6.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been classified as critical. Affected is the function searchTopic of the file wetech-cms- master\wetech- core\src\main\java\tech\ wetech\cms\dao\TopicDao .java. The manipulation of the argument con leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and	N/A	A-CJB-WETE- 201224/99					
CVSSv3 Scoring	Scale 0-1	1-2 2		6-7 7-8	8-9 9-10					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may be used. The vendor was contacted early about this disclosure but did not respond in any way. CVE ID : CVE-2024-12480		
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	12-Dec-2024	6.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been declared as critical. Affected by this vulnerability is the function findUser of the file wetech-cms- master\wetech- core\src\main\java\tech\ wetech\cms\dao\UserDao.j ava. The manipulation of the argument searchValue/gId/rId leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. CVE ID : CVE-2024-12481	N/A	A-CJB-WETE- 201224/100
Relative Path Traversal	12-Dec-2024	4.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been rated as problematic. Affected by this issue is the function backup of the file wetech-cms- master\wetech-basic- common\src\main\java\te ch\wetech\basic\util\Back upFileUtil.java of the component Database Backup Handler. The manipulation of the argument name leads to path traversal: '/filedir'.	N/A 6-7 7-8	A-CJB-WETE- 201224/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. CVE ID : CVE-2024-12482		
Affected Ver	sion(s): 1.1			1	
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	12-Dec-2024	6.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2 and classified as critical. This issue affects the function searchTopicByKeyword of the file wetech-cms- master\wetech- core\src\main\java\tech\ wetech\cms\dao\TopicDao .java. The manipulation of the argument keyword leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	N/A	A-CJB-WETE- 201224/102
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t	12-Dec-2024	6.3	CVE ID : CVE-2024-12479 A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been classified as critical. Affected is the function searchTopic of the file wetech-cms- master\wetech- core\src\main\java\tech\ wetech\cms\dao\TopicDao .java. The manipulation of the argument con leads to	N/A	A-CJB-WETE- 201224/103

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

('Injection')) sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. CVE ID : CVE-2024-12480 Improper Neutralization of Special Elements in output A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been declared as critical. Affected by this vulnerability is the function findUser of the file wetech-core-screwain\java\tech\ wetech\cms\dav0UserDaoj ava. The manipulation of the argument searchValue/gld/rld leads to sql injection. The attack can be launched remotely. The exploit has been disclosere but did not respond in any way. N/A A-CJB-WETE-20124/104 Relative Path 12-Dec-2024 6.3 A vulnerability was found in cjbi wetech-cms- use contacted early about this disclosure but did not respond in any way. N/A A-CJB-WETE-201224/104 Relative Path 12-Dec-2024 4.3 A vulnerability was found in cjbi wetech-cms use contacted early about this disclosure but did not respond in any way. N/A A-CJB-WETE-201224/104 Relative Path 12-Dec-2024 4.3 A vulnerability was found in cjbi wetech-cms use the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. N/A A-CJB-WETE-201224/104 Relative Path 12-Dec-2024 4.3 A vulnerability was found in cjbi wetech-cms use is the function backup of the file wetech-basic-commonysrc/main/java/te ch/wetech/basic/util/Back <t< th=""><th>Weakness</th><th>Publish Date</th><th>CVSSv3</th><th>Description & CVE ID</th><th>Patch</th><th>NCIIPC ID</th></t<>	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements m (1)A vulnerability was found in cjbi wetch-cms 1.0/1.1/1.2. It has been declared as critical. Affected by this vulnerability is the function findUser of the file wetech-cms- master\wetech- core\src\main\java\tech\ wetech\cms\dao\UserDao.j ava. The manipulation of the argument searchValue/gld/rld leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.N/AA-CJB-WETE- 201224/104Relative Path Traversal12-Dec-20244.3A vulnerability was found in cjbi wetech-cms to 1.0/1.1/1.2. It has been rated as problematic. Affected by this issue is the function backup of the file wetech-cms- master\wetech-basic- comon/src/main\java\techN/AA-CJB-WETE- 201224/104Relative Path Traversal12-Dec-20244.3A vulnerability was found in cjbi wetech-cms master\wetech-basic- comon/src/main\java\techN/A				launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not		
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m ('Injection')12-Dec-20246.3cjbi wetech-cms techcence ava. The manipulation of the argument searchValue/gld/rld leads to sql injection. The attack can be launched remotely. 				CVE ID : CVE-2024-12480		
Relative Path Traversal12-Dec-20244.3cjbi wetech-cms 1.0/1.1/1.2. It has been rated as problematic. Affected by this issue is the function backup of the file wetech-cms- master\wetech-basic- common\src\main\java\te ch\wetech\basic\util\Back upFileUtil.java of the component DatabaseN/AA-CJB-WETE- 201224/105	Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t	12-Dec-2024	6.3	cjbi wetech-cms 1.0/1.1/1.2. It has been declared as critical. Affected by this vulnerability is the function findUser of the file wetech-cms- master\wetech- core\src\main\java\tech\ wetech\cms\dao\UserDao.j ava. The manipulation of the argument searchValue/gId/rId leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	N/A	,
	Path	12-Dec-2024	4.3	cjbi wetech-cms 1.0/1.1/1.2. It has been rated as problematic. Affected by this issue is the function backup of the file wetech-cms- master\wetech-basic- common\src\main\java\te ch\wetech\basic\util\Back upFileUtil.java of the	N/A	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Backup Handler. The manipulation of the argument name leads to path traversal: '/filedir'. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. CVE ID : CVE-2024-12482		
Affected Ver	sion(s): 1.2				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	12-Dec-2024	6.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2 and classified as critical. This issue affects the function searchTopicByKeyword of the file wetech-cms- master\wetech- core\src\main\java\tech\ wetech\cms\dao\TopicDao .java. The manipulation of the argument keyword leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. CVE ID : CVE-2024-12479	N/A	A-CJB-WETE- 201224/106
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea	12-Dec-2024	6.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been classified as critical. Affected is the function searchTopic of the file wetech-cms- master\wetech-	N/A	A-CJB-WETE- 201224/107

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Componen t ('Injection')			core\src\main\java\tech\ wetech\cms\dao\TopicDao .java. The manipulation of the argument con leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. CVE ID : CVE-2024-12480		
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	12-Dec-2024	6.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been declared as critical. Affected by this vulnerability is the function findUser of the file wetech-cms- master\wetech- core\src\main\java\tech\ wetech\cms\dao\UserDao.j ava. The manipulation of the argument searchValue/gId/rId leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. CVE ID : CVE-2024-12481	N/A	A-CJB-WETE- 201224/108
Relative Path Traversal CVSSv3 Scoring	12-Dec-2024 Scale 0-1	4.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been rated as problematic. Affected by this issue is the function backup of the file wetech-cms- master\wetech-basic-	N/A 6-7 7-8	A-CJB-WETE- 201224/109 8-9 9-10

Weakness	Publish Date	CVSSv3	Description	& CVE ID	Pat	ch	NCIIPC ID
			common\src\n ch\wetech\bas upFileUtil.java component Dat Backup Handler manipulation o argument name path traversal: The attack may remotely. The e been disclosed and may be use vendor was com about this disclosed	nain\java\te ic\util\Back of the abase r. The f the e leads to '/filedir'. be launched exploit has to the public ed. The ntacted early			
			did not respond				
			CVE ID : CVE-2	024-12482			
Vendor: cla							
Product: cla							
Affected Ver	sion(s): 4.8						
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2024	2.4	A vulnerability problematic wa ClassCMS 4.8. A this vulnerabili unknown funct the file /index.p of the compone Management Pa manipulation o argument URL I cross site script attack can be la remotely. The e been disclosed and may be use CVE ID : CVE-2	as found in affected by ty is an ionality of ohp/admin ent Model age. The f the leads to ting. The aunched exploit has to the public	N/A		A-CLA-CLAS- 201224/110
Vendor: cod	• •	d					
Affected Ver	min_dashboar sion(s): 1.0	u					
Improper Neutralizat	09-Dec-2024	3.5	A vulnerability code-projects A		¹ N/A		A-COD-ADMI- 201224/111
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 v	versions		Dage / 2 of 1127				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Dashboard 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /vendor_management.php. The manipulation of the argument username leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions contradicting product names. CVE ID : CVE-2024-12359		
Product: far	macia				
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	01-Dec-2024	6.3	A vulnerability, which was classified as critical, was found in code-projects Farmacia 1.0. This affects an unknown part of the file /visualizar-produto.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.	N/A	A-COD-FARM- 201224/112
Due due to be			CVE ID : CVE-2024-12007		
	tel_manageme	nt_syster	ll i i i i i i i i i i i i i i i i i i		
Affected Vers Improper Restriction of Operations within the Bounds of	05-Dec-2024	5.3	A vulnerability has been found in code-projects Hotel Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the	N/A	A-COD-HOTE- 201224/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			component Administrator Login Password Handler. The manipulation of the argument Str2 leads to stack-based buffer overflow. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12185		
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-Dec-2024	5.3	A vulnerability was found in code-projects Hotel Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file hotelnew.c of the component Available Room Handler. The manipulation of the argument admin_entry leads to stack- based buffer overflow. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12186	N/A	A-COD-HOTE- 201224/114
Vendor: cod	lezips				
Product: teo	chnical_discuss	sion_foru	m		
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea	12-Dec-2024	7.3	A vulnerability classified as critical was found in Codezips Technical Discussion Forum 1.0. This vulnerability affects unknown code of the file /signuppost.php. The manipulation of the	N/A	A-COD-TECH- 201224/115

 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
m Componen t ('Injection')			argument Username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well. CVE ID : CVE-2024-12484		
Vendor: dat	ax-web_projec	ct			
Product: da	tax-web				
Affected Ver	sion(s): 2.1.1				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	09-Dec-2024	6.3	A vulnerability was found in WeiYe-Jing datax-web 2.1.1. It has been classified as critical. This affects an unknown part of the file /api/job/add/. The manipulation of the argument glueSource leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12358	N/A	A-DAT-DATA- 201224/116
Vendor: De	decms				
Product: de	decms				
Affected Ver	sion(s): * Up to	(excluding	g) 5.7.116		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-Dec-2024	3.5	A vulnerability classified as problematic has been found in DedeCMS 5.7.116. Affected is an unknown function of the file /member/article_add.php. The manipulation of the argument body leads to cross site scripting. It is possible to launch the attack remotely. The exploit	N/A	A-DED-DEDE- 201224/117

 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
			has been disclosed to the public and may be used.		
			CVE ID : CVE-2024-12180		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-Dec-2024	3.5	A vulnerability classified as problematic was found in DedeCMS 5.7.116. Affected by this vulnerability is an unknown functionality of the file /member/uploads_add.php of the component SWF File Handler. The manipulation of the argument mediatype leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	N/A	A-DED-DEDE- 201224/118
			CVE ID : CVE-2024-12181		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-Dec-2024	3.5	A vulnerability, which was classified as problematic, has been found in DedeCMS 5.7.116. Affected by this issue is some unknown functionality of the file /member/soft_add.php. The manipulation of the argument body leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12182	N/A	A-DED-DEDE- 201224/119
Improper Neutralizat ion of Input During Web Page Generation	04-Dec-2024	3.5	A vulnerability, which was classified as problematic, was found in DedeCMS 5.7.116. This affects the function RemoveXSS of the file /plus/carbuyaction.php of the component HTTP POST Request Handler. The	N/A	A-DED-DEDE- 201224/120
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
('Cross-site Scripting')			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.		
Van dam fah	•		CVE ID : CVE-2024-12183		
Vendor: fab		over ca	haduling quatam		
		_exam_sc	heduling_system		
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	12-Dec-2024	6.3	A vulnerability, which was classified as critical, has been found in code-projects Online Class and Exam Scheduling System 1.0. This issue affects some unknown processing of the file /pages/department.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12485	N/A	A-FAB-ONLI- 201224/121
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	12-Dec-2024	6.3	A vulnerability, which was classified as critical, was found in code-projects Online Class and Exam Scheduling System 1.0. Affected is an unknown function of the file /pages/rank_update.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	N/A	A-FAB-ONLI- 201224/122

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-12486		
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	12-Dec-2024	6.3	A vulnerability has been found in code-projects Online Class and Exam Scheduling System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /pages/room_update.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12487	N/A	A-FAB-ONLI- 201224/123
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	12-Dec-2024	6.3	A vulnerability was found in code-projects Online Class and Exam Scheduling System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /pages/subject_update.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12488	N/A	A-FAB-ONLI- 201224/124
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea	12-Dec-2024	6.3	A vulnerability was found in code-projects Online Class and Exam Scheduling System 1.0. It has been classified as critical. This affects an unknown part of the file /pages/term.php. The manipulation of the	N/A	A-FAB-ONLI- 201224/125

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Componen t ('Injection')			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.		
Ware dame Calif			CVE ID : CVE-2024-12489		
Vendor: fabi	lanros line_notice_bo	ard			
Affected Vers					
			A vulnerability was found in		
Improper Access Control	05-Dec-2024	7.3	code-projects Online Notice Board up to 1.0 and classified as critical. This issue affects some unknown processing of the file /registration.php of the component Profile Picture Handler. The manipulation of the argument img leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	N/A	A-FAB-ONLI- 201224/126
			CVE ID : CVE-2024-12233		
Vendor: GFI					
Product: arc					
Affected Vers	sion(s): * Up to	(excluding			
N/A	12-Dec-2024	9.8	GFI Archiver Telerik Web UI Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GFI Archiver. Authentication is not required to exploit this vulnerability.	N/A	A-GFI-ARCH- 201224/127
				I	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The specific flaw exists within the product installer. The issue results from the use of a vulnerable version of Telerik Web UI. An attacker can leverage this vulnerability to execute code in the context of NETWORK SERVICE. Was ZDI-CAN-24041.		
			CVE ID : CVE-2024-11948		
Deserializa tion of Untrusted Data	12-Dec-2024	8.8	GFI Archiver Core Service Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GFI Archiver. Authentication is required to exploit this vulnerability. The specific flaw exists within the Core Service, which listens on TCP port 8017 by default. The issue results from the lack of proper validation of user- supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN- 24029.	N/A	A-GFI-ARCH- 201224/128
			CVE ID : CVE-2024-11947		
Deserializa tion of Untrusted Data	12-Dec-2024	8.8	GFI Archiver Store Service Deserialization of Untrusted Data Remote Code Execution Vulnerability.	N/A	A-GFI-ARCH- 201224/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability allows remote attackers to execute arbitrary code on affected installations of GFI Archiver. Authentication is required to exploit this vulnerability.		
			The specific flaw exists within the Store Service, which listens on TCP port 8018 by default. The issue results from the lack of proper validation of user- supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN- 24331. CVE ID : CVE-2024-11949		
Vendor: Goo Product: ch					
		(ovcludin	a) 121 0 6778 120		
Allected ver	sion(s): [•] op to	(excluding	g) 131.0.6778.139	https://	
Access of Resource Using Incompatib le Type ('Type Confusion')	12-Dec-2024	8.8	Type Confusion in V8 in Google Chrome prior to 131.0.6778.139 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) CVE ID : CVE-2024-12381	https:// chromer eleases.g oogleblo g.com/2 024/12/ stable- channel- update- for- desktop_ 10.html	A-GOO-CHRO- 201224/130
Use After Free	12-Dec-2024	8.8	Use after free in Translate in Google Chrome prior to 131.0.6778.139 allowed a	https:// chromer eleases.g	A-GOO-CHRO- 201224/131

4-5

5-6

6-7

7-8

8-9

9-10

3-4

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) CVE ID : CVE-2024-12382	oogleblo g.com/2 024/12/ stable- channel- update- for- desktop_ 10.html	
	reamer_projec	t			
Product: gs		() I') 1 2 4 4 0		
Affected Ver	sion(s): * Up to	(excluding		1	
Out-of- bounds Write	12-Dec-2024	7.5	GStreamer is a library for constructing graphs of media-handling components. An OOB-write vulnerability has been identified in the gst_ssa_parse_remove_overr ide_codes function of the gstssaparse.c file. This function is responsible for parsing and removing SSA (SubStation Alpha) style override codes, which are enclosed in curly brackets ({}). The issue arises when a closing curly bracket "}" appears before an opening curly bracket "{" in the input string. In this case, memmove() incorrectly duplicates a substring. With each successive loop iteration, the size passed to memmove() becomes progressively larger (strlen(end+1)), leading to a write beyond the allocated memory bounds. This vulnerability is fixed in 1.24.10.	https:// gitlab.fr eedeskt op.org/g streame r/gstrea mer/- /merge_ requests /8036.p atch, https:// gstream er.freed esktop.o rg/secur ity/sa- 2024- 0023.ht ml	A-GST-GSTR- 201224/132

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
			CVE ID : CVE-2024-47541		
Out-of- bounds Read	12-Dec-2024	7.5	GStreamer is a library for constructing graphs of media-handling components. A null pointer dereference has been discovered in the id3v2_read_synch_uint function, located in id3v2.c. If id3v2_read_synch_uint is called with a null work- >hdr.frame_data, the pointer guint8 *data is accessed without validation, resulting in a null pointer dereference. This vulnerability can result in a Denial of Service (DoS) by triggering a segmentation fault (SEGV). This vulnerability is fixed in 1.24.10. CVE ID : CVE-2024-47542	https:// gitlab.fr eedeskt op.org/g streame r/gstrea mer/- /merge_ requests /8033.p atch, https:// gstream er.freed esktop.o rg/secur ity/sa- 2024- 0008.ht ml	A-GST-GSTR- 201224/133
Vendor: IBM	1				
Product: co	gnos_controlle	r			
Affected Ver	sion(s): 11.0.0				
Unrestricte d Upload of File with Dangerous Type	03-Dec-2024	8	IBM Cognos Controller 11.0.0 and 11.0.1 could be vulnerable to malicious file upload by not validating the content of the file uploaded to the web interface. Attackers can make use of this weakness and upload malicious executable files into the system, and it can be sent to victim for performing further attacks.	https:// www.ib m.com/s upport/ pages/n ode/717 7220	A-IBM-COGN- 201224/134

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
			CVE ID : CVE-2024-40691		
Use of Hard- coded Credentials	03-Dec-2024	7.5	IBM Cognos Controller 11.0.0 and 11.0.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. CVE ID : CVE-2024-41777	https:// www.ib m.com/s upport/ pages/n ode/717 7220	A-IBM-COGN- 201224/135
Cross-Site Request Forgery (CSRF)	03-Dec-2024	6.5	IBM Cognos Controller 11.0.0 and 11.0.1	https:// www.ib m.com/s upport/ pages/n ode/717 7220	A-IBM-COGN- 201224/136

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.		
-			CVE ID : CVE-2024-41776 IBM Cognos Controller		
Cleartext Transmissi on of Sensitive Informatio n	03-Dec-2024	5.9	11.0.0 and 11.0.1 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques.	https:// www.ib m.com/s upport/ pages/n ode/717 7220	A-IBM-COGN- 201224/137
			CVE ID : CVE-2021-29892		
Use of a Broken or Risky Cryptograp hic Algorithm	03-Dec-2024	5.9	IBM Cognos Controller 11.0.0 and 11.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. CVE ID : CVE-2024-41775	https:// www.ib m.com/s upport/ pages/n ode/717 7220	A-IBM-COGN- 201224/138
			IBM Cognos Controller 11.0.0 and 11.0.1		
Unrestricte d Upload of File with Dangerous Type	03-Dec-2024	5.5	could be vulnerable to malicious file upload by not validating the type of file uploaded to Journal entry attachments. Attackers can make use of this weakness and upload malicious executable files into the system that can be sent to	https:// www.ib m.com/s upport/ pages/n ode/717 7220	A-IBM-COGN- 201224/139

3-4 4-5

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victims for performing further attacks. CVE ID : CVE-2024-25019		
Unrestricte d Upload of File with Dangerous Type	03-Dec-2024	5.5	IBM Cognos Controller 11.0.0 and 11.0.1 is vulnerable to malicious file upload by allowing unrestricted filetype attachments in the Journal entry page. Attackers can make use of this weakness and upload malicious executable files into the system and can be sent to victims for performing further attacks. CVE ID : CVE-2024-25020	https:// www.ib m.com/s upport/ pages/n ode/717 7220	A-IBM-COGN- 201224/140
Exposure of Sensitive System Informatio n to an Unauthoriz ed Control Sphere	03-Dec-2024	5.3	IBM Cognos Controller 11.0.0 and 11.0.1 exposes server details that could allow an attacker to	https:// www.ib m.com/s upport/ pages/n ode/717 7220	A-IBM-COGN- 201224/141

Authentica tion Bypass Using an Alternate Path or Channel03-Dec-20244.3IBM Cognos Controller 11.0.0 and 11.0.1https:// www.ib m.com/s upport/ pages/n ode/717 7220A-IBM- 201224Ibm Cognos Controller 11.0.0 and 11.0.1A-IBM- upport/ pages/n ode/717 7220A-IBM- 201224Ibm Cognos Controller 11.0.0 and 11.0.1Ibm Cognos m.com/s upport/ pages/n ode/717 7220A-IBM- 201224Ibm Cognos Controller 11.0.0 and 11.0.1Ibm Cognos m.com/s upport/ pages/n ode/717 7220A-IBM- 201224Ibm Cognos Controller 11.0.0 and 11.0.1Ibm Cognos Controller 11.0.0 and 11.0.1Ibm Cognos Controller 11.0.0 and 11.0.1	
Authentica tion Bypass Using an Alternate Path or Channel03-Dec-20244.311.0.0 and 11.0.1https:// www.ib m.com/s upport/ pages/n ode/717 7220A-IBM- 201224Could allow an authenticated user with local access to bypass security allowing users to circumvent restrictions imposed on input fields.https:// authenticated vectorA-IBM- 201224Image: Decemptor of the security allowing users to circumvent restrictions imposed on input fields.The security allowing users to circumvent restrictions imposed on input fields.Images (1000)Image: Decemptor of the security allowing users to circumvent restrictions imposed on input fields.Images (1000)Images (1000)Image: Decemptor of the security allowing users to circumvent restrictions imposed on input fields.Images (1000)Images (1000)Image: Decemptor of the security allowing users to circumvent restrictions imposed on input fields.Images (1000)Images (1000)Image: Decemptor of the security allowing users to circumvent restrictions imposed on input fields.Images (1000)Images (1000)Image: Decemptor of the security allowing users to circumvent restrictions imposed on input fields.Images (1000)Images (1000)Image: Decemptor of the security allowing users to circumvent restrictions imposed on input fields.Images (1000)Images (1000)Image: Decemptor of the security allowing users to circumvent restrictions imposed on input fields.Images (1000)Images (1000)Image: Decemptor of the security allowing users to circumvent restrictions impose	
11.0.0 and 11.0.1 https://	
Insufficient Type Distinction03-Dec-20244.3Main Main 	
Affected Version(s): 11.0.1	
Unrestricte d Upload of File with03-Dec-20248IBM Cognos Controller 11.0.0 and 11.0.1https:// 	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			could be vulnerable to malicious file upload by nor validating the content of th file uploaded to the web interface. Attackers can make use of this weakness and upload malicious executable files into the system, and it can be sent t victim for performing further attacks. CVE ID : CVE-2024-40691	e 7220 o	
Use of Hard- coded Credentials	03-Dec-2024	7.5	IBM Cognos Controller 11.0.0 and 11.0.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. CVE ID : CVE-2024-41777	https:// www.ib m.com/s upport/ pages/n ode/717 7220	A-IBM-COGN- 201224/145
Cross-Site Request Forgery (CSRF)	03-Dec-2024	6.5	IBM Cognos Controller 11.0.0 and 11.0.1	https:// www.ib m.com/s upport/ pages/n	A-IBM-COGN- 201224/146
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
			is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. CVE ID : CVE-2024-41776	ode/717 7220	
Cleartext Transmissi on of Sensitive Informatio n	03-Dec-2024	5.9	IBM Cognos Controller 11.0.0 and 11.0.1 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. CVE ID : CVE-2021-29892	https:// www.ib m.com/s upport/ pages/n ode/717 7220	A-IBM-COGN- 201224/147
Use of a Broken or Risky Cryptograp hic Algorithm	03-Dec-2024	5.9	IBM Cognos Controller 11.0.0 and 11.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. CVE ID : CVE-2024-41775	https:// www.ib m.com/s upport/ pages/n ode/717 7220	A-IBM-COGN- 201224/148
Unrestricte d Upload of	03-Dec-2024	5.5	IBM Cognos Controller 11.0.0 and 11.0.1	https:// www.ib	A-IBM-COGN- 201224/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			could be vulnerable to malicious file upload by not validating the type of file uploaded to Journal entry attachments. Attackers can make use of this weakness and upload malicious executable files into the system that can be sent to victims for performing further attacks. CVE ID : CVE-2024-25019	m.com/s upport/ pages/n ode/717 7220	
Unrestricte d Upload of File with Dangerous Type	03-Dec-2024	5.5	IBM Cognos Controller 11.0.0 and 11.0.1 is vulnerable to malicious file upload by allowing unrestricted filetype attachments in the Journal entry page. Attackers can make use of this weakness and upload malicious executable files into the system and can be sent to	https:// www.ib m.com/s upport/ pages/n ode/717 7220	A-IBM-COGN- 201224/150

Page **61** of **1137**

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victims for performing further attacks.		
			CVE ID : CVE-2024-25020		
			IBM Cognos Controller 11.0.0 and 11.0.1		
Exposure of Sensitive System Informatio n to an Unauthoriz ed Control Sphere	03-Dec-2024	5.3	exposes server details that could allow an attacker to obtain information of the application environment to conduct further attacks. CVE ID : CVE-2024-25035	https:// www.ib m.com/s upport/ pages/n ode/717 7220	A-IBM-COGN- 201224/151
Authentica tion Bypass Using an Alternate Path or Channel	03-Dec-2024	4.3	IBM Cognos Controller 11.0.0 and 11.0.1 could allow an authenticated user with local access to bypass security allowing users to circumvent restrictions imposed on input fields. CVE ID : CVE-2024-25036	https:// www.ib m.com/s upport/ pages/n ode/717 7220	A-IBM-COGN- 201224/152
Insufficient Type Distinction	03-Dec-2024	4.3	IBM Cognos Controller 11.0.0 and 11.0.1	https:// www.ib m.com/s upport/ pages/n ode/717 7220	A-IBM-COGN- 201224/153

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			
			could allow an authenticated user to upload insecure files, due to insufficient file type distinction. CVE ID : CVE-2024-45676					
Vendor: iva	nti			I				
Product: au	tomation							
Affected Ver	sion(s): * Up to	(excluding	g) 2024.4.0.1					
Incorrect Default Permission s	11-Dec-2024	7.8	Under specific circumstances, insecure permissions in Ivanti Automation before version 2024.4.0.1 allows a local authenticated attacker to achieve local privilege escalation. CVE ID : CVE-2024-9845	https://f orums.iv anti.com /s/articl e/Dece mber- 2024- Security - Advisor y-Ivanti- Automat ion-CVE- 2024- 9845	A-IVA-AUTO- 201224/154			
Product: see	Product: security_controls							
Affected Ver	sion(s): * Up to	(excluding	g) 2024.4.1					
Incorrect Default Permission s	11-Dec-2024	7.8	Under specific circumstances, insecure permissions in Ivanti Security Controls before version 2024.4.1 allows a local authenticated attacker to achieve local privilege escalation. CVE ID : CVE-2024-10251	https://f orums.iv anti.com /s/articl e/Securi ty- Advisor y-Ivanti- Security - Controls -iSec- CVE-	A-IVA-SECU- 201224/155			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- 10251	
Product: wo	orkspace_contr	ol			
Affected Vers	sion(s): From (i	ncluding)	10.18.30.0 Up to (excluding) 1	0.18.40.0	
Incorrect Default Permission s	11-Dec-2024	7.8	Under specific circumstances, insecure permissions in Ivanti Workspace Control before version 10.18.40.0 allows a local authenticated attacker to achieve local privilege escalation. CVE ID : CVE-2024-8496	https://f orums.iv anti.com /s/articl e/Dece mber- 2024- Security - Advisor y-Ivanti- Worksp ace- Control- IWC- CVE- 2024- 8496	A-IVA-WORK- 201224/156
Vendor: jwi	llber				•
Product: jfii	nalcms				
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	09-Dec-2024	6.3	A vulnerability was found in JFinalCMS 1.0. It has been rated as critical. Affected by this issue is the function update of the file \src\main\java\com\cms\c ontroller\admin\Template Controller.java of the component Template Handler. The manipulation of the argument content leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	N/A	A-JWI-JFIN- 201224/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-12350		
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	09-Dec-2024	6.3	A vulnerability classified as critical has been found in JFinalCMS 1.0. This affects the function findPage of the file src\main\java\com\cms\e ntity\ContentModel.java of the component File Content Handler. The manipulation of the argument name leads to sql injection. It is possible to initiate the attack remotely. CVE ID : CVE-2024-12351	N/A	A-JWI-JFIN- 201224/158
Cross-Site Request Forgery (CSRF)	09-Dec-2024	4.3	A vulnerability was found in JFinalCMS 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/tag/save. The manipulation leads to cross- site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12349	N/A	A-JWI-JFIN- 201224/159
Vendor: lop	alopa				
Product: e-l	earning_mana	gement_s	ystem		
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Special Elements used in an SQL Command	09-Dec-2024	9.8	A SQL Injection vulnerability was found in /teacher_signup.php of kashipara E-learning Management System v1.0, which allows remote attackers to execute arbitrary SQL command to get unauthorized database	N/A	A-LOP-E-LE- 201224/160
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

		access via the firstname, lastname, and class_id parameters.		
		CVE ID : CVE-2024-54920		
09-Dec-2024	8.8	A SQL Injection vulnerability was found in /search_class.php of kashipara E-learning Management System v1.0, which allows remote attackers to execute arbitrary SQL commands to get unauthorized database access via the school_year parameter. CVE ID : CVE-2024-54926	N/A	A-LOP-E-LE- 201224/161
09-Dec-2024	7.2	KASHIPARA E-learning Management System v1.0 is vulnerable to SQL Injection in /admin/delete_subject.php. CVE ID : CVE-2024-54929	N/A	A-LOP-E-LE- 201224/162
09-Dec-2024	7.2	A SQL Injection was found in /admin/edit_user.php of kashipara E-learning Management System v1.0, which allows remote attackers to execute arbitrary SQL commands to get unauthorized database access via the firstname, lastname, and username parameters. CVE ID : CVE-2024-54922	N/A	A-LOP-E-LE- 201224/163
09-Dec-2024	7.2	Kashipara E-learning Management System v1.0 is vulnerable to SQL Injection	N/A	A-LOP-E-LE- 201224/164
S	09-Dec-2024	09-Dec-2024 7.2 09-Dec-2024 7.2	arbitrary SQL commands to get unauthorized database access via the school_year parameter. CVE ID : CVE-2024-5492609-Dec-20247.2KASHIPARA E-learning Management System v1.0 is vulnerable to SQL Injection in /admin/delete_subject.php. CVE ID : CVE-2024-5492909-Dec-20247.2A SQL Injection was found in /admin/edit_user.php of kashipara E-learning Management System v1.0, which allows remote attackers to execute arbitrary SQL commands to get unauthorized database access via the firstname, lastname, and username parameters. CVE ID : CVE-2024-5492209-Dec-20247.2Kashipara E-learning Management System v1.0, which allows remote attackers to execute arbitrary SQL commands to get unauthorized database access via the firstname, lastname, and username parameters. CVE ID : CVE-2024-5492209-Dec-20247.2Kashipara E-learning Management System v1.0 is vulnerable to SQL Injection	arbitrary SQL commands to get unauthorized database access via the school_year parameter. CVE ID : CVE-2024-5492609-Dec-20247.2KASHIPARA E-learning Management System v1.0 is vulnerable to SQL Injection in /admin/delete_subject.php. CVE ID : CVE-2024-54929N/A09-Dec-20247.2A SQL Injection was found in /admin/delete_subject.php. CVE ID : CVE-2024-54929N/A09-Dec-20247.2A SQL Injection was found in /admin/edit_user.php of kashipara E-learning Management System v1.0, which allows remote attackers to execute arbitrary SQL commands to get unauthorized database access via the firstname,

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		in /admin/delete_student.php. CVE ID : CVE-2024-54930		
09-Dec-2024	7.2	Kashipara E-learning Management System v1.0 is vulnerable to SQL Injection in /admin/delete_content.php. CVE ID : CVE-2024-54933	N/A	A-LOP-E-LE- 201224/165
09-Dec-2024	5.4	A Stored Cross-Site Scripting (XSS) vulnerability was found in /send_message.php of Kashipara E-learning Management System v1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the my_message parameter. CVE ID : CVE-2024-54936	N/A	A-LOP-E-LE- 201224/166
09-Dec-2024	5.4	A Stored Cross Site Scripting (XSS) was found in /teacher_avatar.php of kashipara E-learning Management System v1.0. This vulnerability allows remote attackers to execute arbitrary java script via the filename parameter. CVE ID : CVE-2024-54919	N/A	A-LOP-E-LE- 201224/167
09-Dec-2024	5.4	A Stored Cross-Site Scripting (XSS) vulnerability was found in /send_message_teacher_to_ student.php of kashipara E-	N/A 6-7 7-8	A-LOP-E-LE- 201224/168 8-9 9-10
	09-Dec-2024 09-Dec-2024 09-Dec-2024 09-Dec-2024	09-Dec-2024 7.2 09-Dec-2024 5.4 09-Dec-2024 5.4 09-Dec-2024 5.4	Image: Normal System visual	in /admin/delete_student.php. CVE ID : CVE-2024-5493009-Dec-20247.2Kashipara E-learning Management System v1.0 is vulnerable to SQL Injection in /admin/delete_content.php. CVE ID : CVE-2024-54933N/A09-Dec-20247.2A Stored Cross-Site Scripting (XSS) vulnerability was found in /send_message.php of Kashipara E-learning Management System v1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the my_message parameter. CVE ID : CVE-2024-54936N/A09-Dec-20245.4A Stored Cross Site Scripting (XSS) vulnerability was found in /send_message.php of Kashipara E-learning Management System v1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the my_message parameter. CVE ID : CVE-2024-54936N/A09-Dec-20245.4A Stored Cross Site Scripting (XSS) vulnerability allows remote attackers to execute arbitrary java script via the filename parameter. CVE ID : CVE-2024-54919N/A09-Dec-20245.4A Stored Cross Site Scripting (XSS) vulnerability was found in /send_message_teacher_to_ student.php of kashipara E-N/A

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			learning Management System v1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the my_message parameter.		
			CVE ID : CVE-2024-54935		
N/A	09-Dec-2024	5.3	A Directory Listing issue was found in Kashipara E- Learning Management System v1.0, which allows remote attackers to access sensitive files and directories via /admin/assets. CVE ID : CVE-2024-54937	N/A	A-LOP-E-LE- 201224/169
Vendor: ma	wirik				
	vocate_office_r	nanagom	ont system		
Affected Ver		nanagem	ent_system		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2024	3.5	A vulnerability, which was classified as problematic, has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0. Affected by this issue is some unknown functionality of the file /control/client_data.php. The manipulation of the argument id leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12536	N/A	A-MAY-ADVO- 201224/170
	1				
Product: be	st_house_renta	al_manag	ement_system		

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
External Control of File Name or Path	09-Dec-2024	4.3	A vulnerability was found in SourceCodester Best House Rental Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument page leads to file inclusion. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12357	N/A	A-MAY-BEST- 201224/171
Vendor: onl	ine_class_and_	exam_sch	neduling_system_project	<u> </u>	
Product: on	line_class_and	_exam_sc	heduling_system		
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	09-Dec-2024	6.3	A vulnerability was found in code-projects Online Class and Exam Scheduling System 1.0. It has been rated as critical. This issue affects some unknown processing of the file class_update.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12360	N/A	A-ONL-ONLI- 201224/172
Vendor: ope					
	bot_operating_	system			
Affected Ver	sion(s): 2				
		9.8	Insecure Permissions	N/A	A-OPE-ROBO-
Improper Preservati	06-Dec-2024	7.0	vulnerability in Open		201224/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on of Permission s			Robotics Robotic Operating System 2 ROS2 navigation2 v.humble allows an attacker to execute arbitrary code via the dyn_param_handler_ component.		
			CVE ID : CVE-2024-41644		
Improper Preservati on of Permission s	06-Dec-2024	9.8	Insecure Permissions vulnerability in Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble allows an attacker to execute arbitrary code via a crafted script to the nav2_amcl.	N/A	A-OPE-ROBO- 201224/174
			CVE ID : CVE-2024-41645		
Improper Preservati on of Permission s	06-Dec-2024	9.8	Insecure Permissions vulnerability in Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble allows an attacker to execute arbitrary code via a crafted script to the nav2_dwb_controller.	N/A	A-OPE-ROBO- 201224/175
			CVE ID : CVE-2024-41646 Insecure Permissions		
N/A	06-Dec-2024	9.8	vulnerability in Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble allows an attacker to execute arbitrary code via a crafted script to the nav2_mppi_controller. CVE ID : CVE-2024-41647	N/A	A-OPE-ROBO- 201224/176
Improper Preservati on of Permission s	06-Dec-2024	9.8	Insecure Permissions vulnerability in Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble allows an attacker to execute arbitrary code via a crafted script to the	N/A	A-OPE-ROBO- 201224/177

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nav2_regulated_pure_pursui t_controller.		
			CVE ID : CVE-2024-41648		
Improper Preservati on of Permission s	06-Dec-2024	9.8	Insecure Permissions vulnerability in Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble allows an attacker to execute arbitrary code via a crafted script to the executor_thread CVE ID : CVE-2024-41649	N/A	A-OPE-ROBO- 201224/178
Improper Preservati on of Permission s	06-Dec-2024	9.8	Insecure Permissions vulnerability in Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble allows an attacker to execute arbitrary code via a crafted script to the nav2_costmap_2d. CVE ID : CVE-2024-41650	N/A	A-OPE-ROBO- 201224/179
NULL Pointer Dereferenc e	06-Dec-2024	7.5	Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble was discovered to contain a NULL pointer dereference via the component computeControl(). CVE ID : CVE-2024-44853	N/A	A-OPE-ROBO- 201224/180
NULL Pointer Dereferenc e	06-Dec-2024	7.5	Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble was discovered to contain a NULL pointer dereference via the component smoothPlan(). CVE ID : CVE-2024-44854	N/A	A-OPE-ROBO- 201224/181
NULL Pointer	06-Dec-2024	7.5	Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble was	N/A	A-OPE-ROBO- 201224/182

 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
Dereferenc e			discovered to contain a NULL pointer dereference via the component nav2_navfn_planner(). CVE ID : CVE-2024-44855		
NULL Pointer Dereferenc e	06-Dec-2024	7.5	Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble was discovered to contain a NULL pointer dereference via the component nav2_smac_planner(). CVE ID : CVE-2024-44856	N/A	A-OPE-ROBO- 201224/183
Vendor: php					
	mplaint_mana	gement_s	ystem		
Affected Vers	sion(s): 1.0				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	05-Dec-2024	7.3	A vulnerability classified as critical has been found in PHPGurukul Complaint Management System 1.0. Affected is an unknown function of the file /admin/user-search.php. The manipulation of the argument search 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-2024-12228	N/A	A-PHP-COMP- 201224/184
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen	05-Dec-2024	7.3	A vulnerability classified as critical was found in PHPGurukul Complaint Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/complaint- search.php. The manipulation of the	N/A	A-PHP-COMP- 201224/185
CVSSv3 Scoring	Scale 0-1	1-2 2		6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
t ('Injection')			argument search 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-2024-12229		
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	05-Dec-2024	7.3	A vulnerability, which was classified as critical, has been found in PHPGurukul Complaint Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/subcategory.php. The manipulation of the argument category 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-2024-12230	N/A	A-PHP-COMP- 201224/186
Product: co	vid_19_testing	manager	nent_system		
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2024	6.1	A Reflected Cross Site Scripting (XSS) vulnerability was found in /covidtms/registered-user- testing.php in PHPGurukul COVID 19 Testing Management System 1.0 which allows remote attackers to execute arbitrary code via the regmobilenumber parameter. CVE ID : CVE-2024-55268	N/A	A-PHP-COVI- 201224/187
Vendor: Pro	ogress				
Product: wl	hatsup_gold				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Vers	Affected Version(s): * Up to (excluding) 24.0.1							
N/A	02-Dec-2024	9.8	In WhatsUp Gold versions released before 2024.0.1, a remote unauthenticated attacker could leverage this vulnerability to execute code in the context of the service account. CVE ID : CVE-2024-46909	https:// commun ity.progr ess.com /s/articl e/Whats Up- Gold- Security - Bulletin- Septemb er-2024	A-PRO-WHAT- 201224/188			
Incorrect Use of Privileged APIs	02-Dec-2024	9.8	In WhatsUp Gold versions released before 2024.0.1, a remote unauthenticated attacker could leverage NmAPI.exe to create or change an existing registry value in registry path HKEY_LOCAL_MACHINE\SO FTWARE\WOW6432Node\ Ipswitch\. CVE ID : CVE-2024-8785	https:// commun ity.progr ess.com /s/articl e/Whats Up- Gold- Security - Bulletin- Septemb er-2024	A-PRO-WHAT- 201224/189			
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-2024	8.8	In WhatsUp Gold versions released before 2024.0.1, a SQL Injection vulnerability allows an authenticated lower-privileged user (at least Network Manager permissions required) to achieve privilege escalation to the admin account. CVE ID : CVE-2024-46905	https:// commun ity.progr ess.com /s/articl e/Whats Up- Gold- Security - Bulletin- Septemb er-2024	A-PRO-WHAT- 201224/190			
Improper Neutralizat	02-Dec-2024	8.8	In WhatsUp Gold versions released before 2024.0.1, a	https:// commun	A-PRO-WHAT- 201224/191			

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		
ion of Special Elements used in an SQL Command ('SQL Injection')			SQL Injection vulnerability allows an authenticated low-privileged user (at least Report Viewer permissions required) to achieve privilege escalation to the admin account. CVE ID : CVE-2024-46906	ity.progr ess.com /s/articl e/Whats Up- Gold- Security - Bulletin- Septemb er-2024			
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-2024	8.8	In WhatsUp Gold versions released before 2024.0.1, a SQL Injection vulnerability allows an authenticated low-privileged user (at least Report Viewer permissions required) to achieve privilege escalation to the admin account. CVE ID : CVE-2024-46907	https:// commun ity.progr ess.com /s/articl e/Whats Up- Gold- Security - Bulletin- Septemb er-2024	A-PRO-WHAT- 201224/192		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-2024	8.8	In WhatsUp Gold versions released before 2024.0.1, a SQL Injection vulnerability allows an authenticated low-privileged user (at least Report Viewer permissions required) to achieve privilege escalation to the admin account. CVE ID : CVE-2024-46908	https:// commun ity.progr ess.com /s/articl e/Whats Up- Gold- Security - Bulletin- Septemb er-2024	A-PRO-WHAT- 201224/193		
Vendor: razormist							
-	one_contact_m	anager_s	ystem				
Affected Vers	sion(s): 1.0						

0-1

1-2

2-3

5-6

6-7

9-10

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Dec-2024	5.3	A vulnerability, which was classified as critical, was found in SourceCodester Phone Contact Manager System 1.0. Affected is the function UserInterface::MenuDisplay Start of the component User Menu. The manipulation leads to buffer overflow. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12354	N/A	A-RAZ-PHON- 201224/194
Improper Input Validation	09-Dec-2024	3.3	A vulnerability, which was classified as problematic, has been found in SourceCodester Phone Contact Manager System 1.0. This issue affects the function UserInterface::MenuDisplay Start of the component User Menu. The manipulation of the argument name leads to improper input validation. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12353	N/A	A-RAZ-PHON- 201224/195
Improper Input Validation CVSSv3 Scoring	09-Dec-2024	3.3	A vulnerability has been found in SourceCodester Phone Contact Manager System 1.0 and classified as problematic. Affected by this vulnerability is the function ContactBook::adding of the file ContactBook.cpp. The manipulation leads to	N/A 6-7 7-8	A-RAZ-PHON- 201224/196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper input validation. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used.		
			CVE ID : CVE-2024-12355		
Vendor: Ro	ckwellautomat	tion			
Product: ar	ena_simulation	1			
Affected Ver	sion(s): * Up to	(including	g) 16.20.03		
Out-of- bounds Write	05-Dec-2024	7.8	An "out of bounds write" code execution vulnerability exists in the Rockwell Automation Arena® that could allow a threat actor to write beyond the boundaries of allocated memory in a DOE file. If exploited, a threat actor could leverage this vulnerability to execute arbitrary code. To exploit this vulnerability, a legitimate user must execute the malicious code crafted by the threat actor. CVE ID : CVE-2024-11156	https:// www.ro ckwellau tomatio n.com/e n- us/trust - center/s ecurity- advisori es/advis ory.SD1 713.htm l	A-ROC-AREN- 201224/197
Out-of- bounds Read	05-Dec-2024	7.8	An "out of bounds read" code execution vulnerability exists in the Rockwell Automation Arena® that could allow a threat actor to craft a DOE file and force the software to read	https:// www.ro ckwellau tomatio n.com/e n- us/trust - center/s ecurity-	A-ROC-AREN- 201224/198

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
			beyond the boundaries of an allocated memory. If exploited, a threat actor could leverage this vulnerability to execute arbitrary code. To exploit this vulnerability, a legitimate user must execute the malicious code crafted by the threat actor. CVE ID : CVE-2024-12130	advisori es/advis ory.SD1 713.htm l	
Vendor: ujc	ms				
Product: ujo					
Affected Vers	sion(s): * Up to	(excluding	g) 9.6.3		
Improper Authorizati on	12-Dec-2024	3.7	A vulnerability classified as problematic has been found in Dromara UJCMS up to 9.6.3. This affects an unknown part of the file /users/id of the component User ID Handler. The manipulation leads to authorization bypass. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12483	N/A	A-UJC-UJCM- 201224/199
			Hardware		
Vendor: Qua	alcomm				
Product: 20	5_mobile_plat	form			
Affected Vers	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro	H-QUA-205 201224/200
CVSSv3 Scoring *stands for all v		1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-205 201224/201
	5_mobile_plat	form			
Affected Ver	sion(s): -				
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-215 201224/202
Product: 31 Affected Ver	5_5g_iot_mode	m			
	31011(3).				

Validation of Array Index02-Dec-20248.4Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044Differes/ urces/se urces/se urtybu lletin/de comber- 2024- bulletin. httmlH-QUA-315 201224/203Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu bliftereso urces/se urces/se curitybu letin/de cember- 2024- bulletin. httmlH-QUA-315 201224/204Product: 9205_Ite_modemMemory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu bliftereso urces/se curitybu letin/de cember- 2024- bulletin. httmlH-QUA-315 201224/204Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056H-QUA-9205- 201224/204Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu bliftereso urces/se curitybu llcem.htmlProduct: 9206_Ite_modem911223344556677.88.9910	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056docs.qua lcomm.c on/pro duct/pu lletin/de cember- 2024- builetin. htmlH-QUA-315 201224/204Product: 920-2-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition htmlhttps:// docs.qua letin/de cember- 2024- builetin. htmlH-QUA-315 201224/204Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se urces/se comber- 2024- builetin. htmlProduct: 9205_Ite_modem12233445566-77889940	Improper Validation of Array Index	02-Dec-2024	8.4	Configuring the SMR/S2CR register in Bypass mode.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	• –		
Affected Version(s): - Affected Version(s): - Buffer 02-Dec-2024 8.4 Memory corruption when allocating and accessing an entry in an SMEM partition continuously. https:// docs.qua lcomm.c memory corruption when allocating and accessing an entry in an SMEM partition continuously. H-QUA-9205-201224/205 Ver ID : CVE ID : CVE-2024-33056 CVE ID : CVE-2024-33056 H-QUA-9205-201224/205 Product: 92U6_Ite_modem Uestion of the modem H-QUA-9205-201224/205 CVSSV3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7.8 8-9 910	Buffer Over-read	02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•		
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlH-QUA-9205- 201224/205Product: 9205- 201224/205CVSSV3 Scoring Scale0-11-22-33-44-55-66-77-88-99-10	Product: 92	05_lte_modem	L					
Buffer Over-read02-Dec-20248.4Remory corruption when allocating and accessing an entry in an SMEM partition CVE ID : CVE-2024-33056docs.qua lcom.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlH-QUA-9205- 012224/205Product: 92/Dec-2024Remory corruption when allocating and accessing an entry in an SMEM partition CVE ID : CVE-2024-33056docs.qua lcom.re om/pro 	Affected Ver	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	Buffer Over-read	02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	÷		
	Product: 9206_lte_modem							
stands for all versions			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 Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-9206- 201224/206
Product: 92	07_lte_modem	l			
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-9207- 201224/207
Product: ap	q8017				I
Affected Ver	sion(s): -				
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-APQ8- 201224/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
				2024- bulletin. html						
Product: ap	Product: apq8037									
Affected Ver	sion(s): -									
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-APQ8- 201224/209					
Product: aq	t1000									
Affected Ver	sion(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-AQT1- 201224/210					
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-AQT1- 201224/211					

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			
				lletin/de cember- 2024- bulletin. html				
Product: ar	8035							
Affected Ver	sion(s): -			1				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-AR80- 201224/212			
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-AR80- 201224/213			
Product: c-w	/2x_9150							
Affected Version(s): -								
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-C-V2- 201224/214			

		to huge allocation or invalid	urces/se					
		memory access. CVE ID : CVE-2024-33036	curitybu lletin/de cember- 2024- bulletin. html					
02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-C-V2- 201224/215				
02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-C-V2- 201224/216				
Product: csrb31024								
Affected Version(s): -								
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-CSRB- 201224/217				
	02-Dec-2024 rb31024 sion(s): -	02-Dec-2024 6.1 o2-Dec-2024 6.1 o2-Dec-2024 8.4	02-Dec-20246.7multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-3305302-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-33037cb31024sion(s): -02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053docs.qua icom/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html02-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-33037https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin. httmlrb31024Memory corruption while COFiguring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin.de cember-2024- bulletin.				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybu lletin/de cember- 2024- bulletin. html	
	stconnect_6200)			
Affected Ver	sion(s): -				[
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/218
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/219
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-FAST- 201224/220

Stack-based 02-Dec-2024 7.8 Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. https:// docs.qua lcomm.c I-QUA-FAST-201224/221 Use After Pree 02-Dec-2024 6.7 Memory corruption when multiple threads try to unregister the CVP buffer at the same time. https:// docs.qua lcomm.c I-QUA-FAST-201224/221 Use After Free 02-Dec-2024 6.7 Memory corruption when multiple threads try to unregister the CVP buffer at the same time. https:// docs.qua lcomm.c I-QUA-FAST-201224/221 Memory corruption when multiple threads try to unregister the CVP buffer at the same time. https:// docs.qua lcomm.c I-QUA-FAST-201224/222 Memory corruption when multiple threads try to unregister the CVP buffer at the same time. https:// docs.qua lcomm.c I-QUA-FAST-201224/222 Memory corruption while configuring the SMR/S2CR register in Bypass mode. IteQUA-FAST-201224/222 II-QUA-FAST-201224/222 Improper Validation index 02-Dec-2024 8.4 Memory corruption while configuring the SMR/S2CR register in Bypass mode. https:// docs.qua lcomm.c Improper Validation index 02-Dec-2024 8.4 Memory corruption while configuring the SMR/S2CR register in Bypass mode. https:// docs.qua lcomm.c indu2/4/223 Improper Validation index 02-Dec-2024 8.4<	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based based Buffer Overflow02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050docs.qua loc out/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlH-QUA-FAST- 201224/221Use After Free02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua lcomm.c multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua lcomm.c multiple threads try to unregister the CVP buffer at lletin/de cember- 2024- bulletin. htmlhttps:// docs.qua lcomm.c multiple threads try to unregister the CVP buffer at lletin/de cember- 2024- bulletin. htmlhttps:// docs.qua lcomm.c multiple threads try to unregister the CVP buffer at lletin/de cember- 2024- bulletin. htmlhttps:// docs.qua lcomm.c the same time. CVE ID : CVE-2024-33053https:// docs.qua lcomm.c the same time. CVE ID : CVE-2024-33054https:// docs.qua lcomm.c the same time. letin/de cember- 2024- bulletin. htmlImproper Validation index02-Dec-20248.4Memory corruption while configuring the SMR/S2CR register in Bypass mode. UCK ID : CVE-2024-33044https:// docs.qua lcomm.c duct/pu blicreso urces/se urces/sehttps:// docs.qua lcomm.c tot.pu blicreso urces/sehttps:// docs.qua lcomm.c					cember- 2024- bulletin.	
Use After Free02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053docs.qua lcomm.c 	based Buffer	02-Dec-2024	7.8	invoking IOCTL calls from user space to issue factory test command inside WLAN driver.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•
Affected Version(s): -Improper Validation of Array Index02-Dec-20248.4Nemory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/deH-QUA-FAST- 201224/223		02-Dec-2024	6.7	multiple threads try to unregister the CVP buffer at the same time.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua Icomm.c om/pro blicreso urces/se curitybu lletin/deH-QUA-FAST- 201224/223CVSSv3 Scoring Scale0-11-22-33-44-55-66-77-88-99-10	Product: fas	stconnect_6700)		I	
Improper Validation of Array Index 02-Dec-2024 8.4 Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044 docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de H-QUA-FAST- 201224/223	Affected Ver	sion(s): -				
	Validation of Array	02-Dec-2024	8.4	Configuring the SMR/S2CR register in Bypass mode.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	•
			1-2 2	<mark>-3 3-4 4-5 5-6</mark>	6-7 7-8	8-9 9-10

		CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/224
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/225
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/227
	stconnect_680)			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/228
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/229

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/230
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/231
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/232
Use After Free CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-FAST- 201224/233 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html					
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/234				
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/235				
	Product: fastconnect_6900 Affected Version(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-FAST- 201224/236				
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
				blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	urces/se curitybu	H-QUA-FAST- 201224/237
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-4304 8	curitybu	H-QUA-FAST- 201224/238
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-FAST- 201224/239
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
				cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/240
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/241
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/243
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/244
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/245
Use After Free CVSSv3 Scoring	02-Dec-2024 Scale 0-1	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-FAST- 201224/246 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33053	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/247
Product: fas	stconnect_7800)		L	
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/248
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-FAST- 201224/249

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CV	'E ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-	·33056	blicresc urces/s curitybu lletin/d cember 2024- bulletin html	e u e -
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption invalid input is pass invoke GPU Headroo call. CVE ID : CVE-2024-	ed to om API	https:// docs.qu lcomm.c om/pro duct/pu blicresc urces/s curitybu lletin/d cember 2024- bulletin html	a c h H-QUA-FAST- 201224/250 e -
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption invoking IOCTL calls user space to set gen private command in WLAN driver. CVE ID : CVE-2024-	s from neric iside	https:// docs.qu lcomm.c om/pro duct/pu blicresc urces/s curitybu lletin/d cember 2024- bulletin html	a c h H-QUA-FAST- 201224/251 e -
Stack- based Buffer Overflow CVSSv3 Scoring	02-Dec-2024 Scale 0-1	7.8	Memory corruption invoking IOCTL calls user space to issue f test command inside driver. CVE ID : CVE-2024-	s from Factory e WLAN • 43050	https:// docs.qu lcomm.a om/pro duct/pu blicresc urces/s curitybu lletin/d	a c H-QUA-FAST- 201224/252 e u

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/253
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/254
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/256
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FAST- 201224/257
Product: flig	ght_rb5_5g_pla	tform			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FLIG- 201224/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FLIG- 201224/259
Product: fsr	n10055				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-FSM1- 201224/260
Product: fsr	n10056				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-FSM1- 201224/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
				bulletin. html						
Product: ho	Product: home_hub_100_platform									
Affected Ver	sion(s): -									
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-HOME- 201224/262					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-HOME- 201224/263					
Product: im	mersive_home	_214_pla	tform							
Affected Ver	sion(s): -									
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-IMME- 201224/264					

2-3

3-4

4-5

5-6

6-7

7-8

8-9

9-10

CVSSv3 Scoring Scale *stands for all versions

0-1

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				cember- 2024- bulletin. html				
Product: im	mersive_home	_216_pla	tform					
Affected Vers	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IMME- 201224/265			
Product: im	mersive_home	_316_pla	tform					
Affected Vers	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IMME- 201224/266			
	Product: immersive_home_318_platform							
Affected Ver	sion(s): -			1-				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-IMME- 201224/267			
CVSSv3 Scoring *stands for all v		1-2 2	- <mark>3</mark> 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-2024-33056	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html				
	mersive_home	e_3210_pl	atform					
Affected Ver	sion(s): -			-				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IMME- 201224/268			
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IMME- 201224/269			
Product: immersive_home_326_platform								
Affected Version(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https:// docs.qua lcomm.c	H-QUA-IMME- 201224/270			

CVSSv3 Scoring Scale0-11-22-33-44-55-66-7*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IMME- 201224/271
Product: ipo	q5010			I	
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ5- 201224/272
Product: ipo	q5028			•	
Affected Ver	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ5- 201224/273		
Product: ipo	q5300						
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ5- 201224/274		
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ5- 201224/275		
Product: ipq5302							
CVSSv3 Scoring		1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		
*stands for all v	rersions		Page 103 of 1137				

Affected Version(s): - Affected Version(s): - Integer Buffer 02-Dec-2024 8.4 Memory corruption when allocating and accessing an entry in an SMEM partition continuously. Integer Over-read 02-Dec-2024 8.4 Memory corruption when allocating and accessing an entry in an SMEM partition continuously. H-QUA-IPQ5-201224/276 Product: ipq5312 CVE ID : CVE-2024-33056 Integer Https:// doc.s.qua lcomm.c Buffer 02-Dec-2024 8.4 Memory corruption when allocating and accessing an entry in an SMEM partition continuously. H-QUA-IPQ5-201224/276 Buffer 02-Dec-2024 8.4 Memory corruption when allocating and accessing an entry in an SMEM partition continuously. Integer Over-read 02-Dec-2024 8.4 Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an continuously. CVE ID : CVE-2024-33056docs.qua lcomm.c. om/pro urces/se curitybuI-QUA-IPQ5- 201224/276Product: ipq5312EEEAffected Version(s): -Intrashttps:// docs.qua lcomm.c. om/pro docs.qua lcomm.c. om/pro docs.qua lcomm.c. om/pro docs.qua lcomm.c. om/pro urces/se curitybuIntrasIntrasBuffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c. om/pro urces/se curitybuI-QUA-IPQ5- 2024- bulletin. https:// docs.qua lcomm.c. om/pro urces/se curitybuI-QUA-IPQ5- 2024- bulletin.Integer Overflow or Wraparoun d02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater this element is present. Itelin/de cember- 2024- bulletin.I-QUA-IPQ5- 201224/277	Affected Version(s): -						
Affected Version(s): -Affected Version(s): -Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.Liteger Overflow or Wraparoun d02-Dec-20247.5Integer Wraparoun d02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.H-QUA-IPQ5- 201224/277201224/277H-QUA-IPQ5- 201224/277201224/277H-QUA-IPQ5- 201224/277Liteger Overflow or Wraparoun d02-Dec-20247.5CVE ID : CVE-2024-33063CVE ID : CVE-2024-33063		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	• •	
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httmlH-QUA-IPQ5- 201224/277Integer Overflow or Wraparoun d02-Dec-20248.4Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 201224/277	Product: ipo	q5312					
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlH-QUA-IPQ5- 201224/277Integer Overflow or wraparoun d02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	Affected Ver	sion(s): -					
Integer Overflow or d02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/deH-QUA-IPQ5- 201224/278		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.		
2024- bulletin. html	Overflow or Wraparoun	02-Dec-2024	7.5	parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Product: ipe	Product: ipq5332							
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ5- 201224/279			
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ5- 201224/280			
Product: ipe	q6000			•				
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-IPQ6- 201224/281			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
				bulletin. html			
Product: ip	q6005						
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ6- 201224/282		
Product: ip	q6010						
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ6- 201224/283		
Product: ipq6018							
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-IPQ6- 201224/284		
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				
				curitybu lletin/de cember- 2024- bulletin. html					
Product: ipe	Product: ipq6028								
Affected Ver	sion(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ6- 201224/285				
Product: ip	q8064								
Affected Ver	sion(s): -								
				https:// docs.qua lcomm.c					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ8- 201224/286				
		8.4	allocating and accessing an entry in an SMEM partition continuously.	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	• •				
Over-read	q8065	8.4	allocating and accessing an entry in an SMEM partition continuously.	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	• •				
Over-read Product: ipo	q8065	8.4	allocating and accessing an entry in an SMEM partition continuously.	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	• •				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: ip	<u> </u>				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ8- 201224/288
Product: ip	q8070				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ8- 201224/289
Product: ipo	q8070a				
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 v					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Ver	Affected Version(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ8- 201224/290			
Product: ipe	•							
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ8- 201224/291			
Product: ipe	q8071a							
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-IPQ8- 201224/292			

 CVSSv3 Scoring Scale
 0-1
 1-2
 2-3
 3-4

 *stands for all versions

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				2024- bulletin. html				
Product: ipo	18072			1				
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ8- 201224/293			
Product: ipo	Product: ipq8072a							
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ8- 201224/294			
Product: ipq8074								
Affected Version(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-IPQ8- 201224/295			
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		
				urces/se curitybu lletin/de cember- 2024- bulletin. html			
Product: ipo							
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ8- 201224/296		
Product: ip	q8076						
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ8- 201224/297		
Product: ipq8076a							
meeteu vel	Affected Version(s): -						

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ8- 201224/298
Product: ip	•				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ8- 201224/299
Product: ip	q8078a				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-IPQ8- 201224/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
				bulletin. html			
Product: ip	q8173						
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ8- 201224/301		
Product: ip	q8174						
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ8- 201224/302		
Product: ipq9008							
Affected Ver	sion(s): -			1-			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-IPQ9- 201224/303		
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
				curitybu lletin/de cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ9- 201224/304
Product: ipe	q9554				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ9- 201224/305
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-IPQ9- 201224/306

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
				lletin/de cember- 2024- bulletin. html	
Product: ipo	19570			• •	
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ9- 201224/307
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ9- 201224/308
Product: ipo	9574				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-IPQ9- 201224/309

02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	urces/se curitybu lletin/de cember- 2024- bulletin. html https:// docs.qua lcomm.c om/pro duct/pu blicreso					
)2-Dec-2024	7.5	parsing the ML IE when a beacon with common info length of the ML IE greater	docs.qua lcomm.c om/pro duct/pu blicreso					
		than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-IPQ9- 201224/310				
Product: mdm8207								
on(s): -			1					
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-MDM8- 201224/311				
n9205s								
on(s): -			1					
)2-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro	H-QUA-MDM9- 201224/312				
n D:	<mark>9205s</mark> n(s): -	9205s n(s): -	2-Dec-20248.4allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-330569205sn(s): -2-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition	2-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html9205sallocating and accessing an entry in an SMEM partitionallocating and accessing an entry in an SMEM partition				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: md	lm9250				
Affected Vers	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-MDM9- 201224/313
Product: md	lm9628				
Affected Vers	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-MDM9- 201224/314
Product: md	lm9650				
Affected Vers	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-MDM9- 201224/315			
Product: ms	sm8108							
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-MSM8- 201224/316			
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-MSM8- 201224/317			
Product: ms	Product: msm8209							
CVSSv3 Scoring		1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10			
*stands for all v	rersions		Page 118 of 1137					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-MSM8- 201224/318
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-MSM8- 201224/319
Product: ms	m8608				
Affected Vers	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-MSM8- 201224/320
CVSSv3 Scoring *stands for all v		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			
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-MSM8- 201224/321			
Product: ms	sm8909w							
Affected Ver	sion(s): -							
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-MSM8- 201224/322			
	Product: pm8937							
Affected Ver	sion(s): -			I				
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-PM89- 201224/323			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
				bulletin. html			
Product: pn	np8074						
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-PMP8- 201224/324		
Product: qam8255p							
Affected Ver	sion(s): -						
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/325		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-QAM8- 201224/326		

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
				cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/327
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/328
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Product: qam8295p								
Affected Ver	sion(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/330			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/331			
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/332			

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/333
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/334
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/335
Product: qa	-				
Affected Ver	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/336
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/337
Product: qa	m8650p			1	
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/339
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/340
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/341
Product: qa	-		l		
Affected Vers	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/342
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/343
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAM8- 201224/344
Untrusted Pointer Dereferenc e CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the -3 3-4 4-5 5-6	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-QAM8- 201224/345 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handle is not validated by the service. CVE ID : CVE-2024-33039	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qa	msrv1h				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAMS- 201224/346
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAMS- 201224/347
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https:// docs.qua lcomm.c om/pro duct/pu 6-7 7-8	H-QUA-QAMS- 201224/348 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAMS- 201224/349
Product: qa					
Affected Ver	sion(s): -			ſ	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAMS- 201224/350
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-QAMS- 201224/351

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			urces/se curitybu lletin/de cember- 2024- bulletin. html				
02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAMS- 201224/352			
02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QAMS- 201224/353			
Product: qca0000							
Affected Version(s): -							
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-QCA0- 201224/354			
	02-Dec-2024 02-Dec-2024 02-Dec-2024	• •	O2-Dec-2024Image: A mathematical and the service of the	02-Dec-2024Image: Constraint of the service of the servi			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				curitybu lletin/de cember- 2024- bulletin. html				
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA0- 201224/355			
Product: qca1062								
Affected Vers	sion(s): -							
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA1- 201224/356			
Product: qca1064								
Affected Version(s): -								
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver.	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-QCA1- 201224/357			
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10			

Stack- based Buffer Overflow02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybuVerflow02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050https:// docs.qua lcomm.c oduct/pu blicreso urces/se curitybu lletin/de cember-						
Affected Version(s): - Affected Version(s): - Affected Version(s): - https:// https:// docs.qua lcomm.c om/pro based Buffer Overflow 02-Dec-2024 7.8 Memory corruption while invoking IOCTL calls from bicreso user space to issue factory test command inside WLAN driver. EVEND - CVE 2024						
Stack- based Buffer Overflow02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/deH-QUA-QC 201224/3						
Stack- based Buffer Overflow02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver.om/pro duct/pu blicreso urces/se curitybu lletin/deH-QUA-QC 201224/3						
2024- bulletin. html						
Improper Restriction of Operations within the Bounds of a Memory 						
Product: qca2064						
Affected Version(s): -						
Stack- based02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factoryhttps:// docs.qua lcomm.cH-QUA-QC 201224/3						

CVSSv3 Scoring Scale0-11-22-33-44-55-66-7*stands for all versions

7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			test command inside WLAN driver. CVE ID : CVE-2024-43050	om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA2- 201224/361
Product: qc					
Affected Ver	sion(s): -			1	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA2- 201224/362
Improper Restriction of Operations	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN	https:// docs.qua lcomm.c om/pro	H-QUA-QCA2- 201224/363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
within the Bounds of a Memory Buffer			target diagnostic information. CVE ID : CVE-2024-43053	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html				
Product: qc	a2066			·				
Affected Ver	sion(s): -							
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA2- 201224/364			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA2- 201224/365			
Product: qc	Product: qca4004							
Affected Ver	sion(s): -			-				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https:// docs.qua	H-QUA-QCA4- 201224/366			
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qc	a4024			<u> </u>	
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA4- 201224/367
Product: qc	a6164				
Affected Ver	sion(s): -				
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Product: qc	Product: qca6174							
Affected Ver	sion(s): -							
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/369			
Product: qc	a6174a							
Affected Ver	sion(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/370			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-QCA6- 201224/371			

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/372
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/373
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/374
Product: qc	a6310			1	
CVSSv3 Scoring		1-2 2	<mark>-3</mark> 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	Affected Version(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/375			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/376			
Product: qca	a6320							
Affected Vers	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/377			
CVSSv3 Scoring *stands for all v		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: qc	a6335	I			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/378
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/379
Product: qc	a6391			, 	
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-QCA6- 201224/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/381
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/382
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/384
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/385
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/386
Use After Free CVSSv3 Scoring	02-Dec-2024 Scale 0-1	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-QCA6- 201224/387 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33053	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/388
Product: qc	a6420				
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/389
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-QCA6- 201224/390

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/391
Product: qc					
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/392
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-QCA6- 201224/393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/394
Product: qc	a6426				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/395
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-QCA6- 201224/396

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
				curitybu lletin/de cember- 2024- bulletin. html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/397
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/398
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-QCA6- 201224/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/400
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/401
Product: qc					
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-QCA6- 201224/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Product: qc	a6430				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/403
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/404
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-QCA6- 201224/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Product: qc	a6431				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/406
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/407
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-QCA6- 201224/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Product: qc	a6436				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/409
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/410
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-QCA6- 201224/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/412
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/413
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/415
Product: qc	a6438				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/416
Product: qc	a6554a				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-QCA6- 201224/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/418
Product: qc					
Affected Ver	sion(s): -		Г	I	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/419
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-QCA6- 201224/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Product: qc	a6564a				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/421
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/422
Product: qc	a6564au				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-QCA6- 201224/423

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/424
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/425
Product: qc					
Affected Ver	sion(s): -			h44 //	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-QCA6- 201224/426
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3 3-4 4-5 5-6</mark>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/427
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/428
Product: qc	a6574a				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-QCA6- 201224/429
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
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/430
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/431
Product: qc					
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-QCA6- 201224/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/433
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/434
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/435

3-4 4-5

5-6

6-7

8-9

9-10

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/436
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/437
Product: qc	a6584au				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/439
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/440
Product: qc	a6595				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/441

 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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/442
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/443
Product: qc	a6595au				
Affected Ver	sion(s): -			-	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/444

 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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/445
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/446
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/447
Use After Free CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-QCA6- 201224/448 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qc	a6678aq			L	
Affected Vers	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/449
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/450
Integer Overflow or Wraparoun d CVSSv3 Scoring	02-Dec-2024 Scale 0-1	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater -3 3-4 4-5 5-6	https:// docs.qua lcomm.c om/pro duct/pu 6-7 7-8	H-QUA-QCA6- 201224/451 8-9 9-10

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/452
a6688aq				
sion(s): -			1	
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/453
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-QCA6- 201224/454
	02-Dec-2024 02-Dec-2024 02-Dec-2024	02-Dec-2024 6.7 a6688aq	Image: Normal Science of Contract of C	02-Dec-20248.4Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040blicreso urces/se curitybu letin/de cember- 2024- bulletin. httml02-Dec-20248.4Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040https:// docs.qua letin/de cember- 2024- bulletin. html02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua letin/de cember- 2024- bulletin. html02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua letin/de cember- 2024- bulletin. html02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua letin/de cember- 2024- bulletin. html02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua locating and accessing an entry in an SMEM partition docs.qua locating and accessing an entry in an SMEM partition

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
				urces/se curitybu lletin/de cember- 2024- bulletin. html			
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/455		
Product: qca	a6694						
Affected Vers	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/456		
Product: qca6696							
Affected Vers	sion(s): -						
Improper Validation	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode.	https:// docs.qua lcomm.c	H-QUA-QCA6- 201224/457		
of Array Index			CVE ID : CVE-2024-33044	om/pro	,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/458
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/459
Use of Out- of-range Pointer Offset CVSSv3 Scoring	02-Dec-2024 Scale 0-1	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access.	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu 6-7 7-8	H-QUA-QCA6- 201224/460 8-9 9-10

Use After Free02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybuH-QUA- 201224Buffer Over-read02-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-33037https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	0046-
Use After Free02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlH-QUA- 201224Buffer Over-read02-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-33037https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	0046-
Buffer Over-read02-Dec-20246.1Information disclosure as NPU firmware can send driver as the driver doesn't validate the IPC message received from the firmware.docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de 201224	e
html	-
Product: qca6698aq	
Affected Version(s): -	
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode.https:// docs.qua lcomm.c duct/pu blicreso urces/se curitybu lletin/deH-QUA- 201224	•
CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 *stands for all versions	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/464
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/465
Product: qc					
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-QCA6- 201224/466
CVSSv3 Scoring *stands for all v		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
				2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/467
Product: qc	a6787aq				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/468
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-QCA6- 201224/469

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
				bulletin. html	
Product: qc	a6797aq				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/470
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA6- 201224/471
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-QCA6- 201224/472

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
				bulletin. html					
Product: qc	Product: qca8072								
Affected Ver	sion(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA8- 201224/473				
Product: qc	a8075								
Affected Ver	sion(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA8- 201224/474				
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-QCA8- 201224/475				

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Product: qc					
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA8- 201224/476
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA8- 201224/477
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-QCA8- 201224/478

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		
				2024- bulletin. html			
Product: qca	a8082						
Affected Vers	sion(s): -						
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA8- 201224/479		
Product: qca	a8084						
Affected Vers	sion(s): -						
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA8- 201224/480		
Product: qca8085							
Affected Version(s): -							
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-QCA8- 201224/481		
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
			than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qc	a8337				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA8- 201224/482
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA8- 201224/483
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-QCA8- 201224/484

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			
			to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	curitybu lletin/de cember- 2024- bulletin. html				
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA8- 201224/485			
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA8- 201224/486			
	Product: qca8386 Affected Version(s): -							
miected vers	301(3)		Transient DOS while	https://				
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-QCA8- 201224/487			
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
				lletin/de cember- 2024- bulletin. html			
Product: qc	a9377						
Affected Ver	sion(s): -			1			
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA9- 201224/488		
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCA9- 201224/489		
Product: qc	a9379	<u> </u>		I			
Affected Version(s): -							
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-QCA9- 201224/490		

 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
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qc	c2073				
Affected Ver	sion(s): -				
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCC2- 201224/491
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCC2- 201224/492
Improper Restriction of Operations within the Bounds of	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-QCC2- 201224/493

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer				curitybu lletin/de cember- 2024- bulletin. html	
Product: qc					
Affected Ver	sion(s): -			1	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCC2- 201224/494
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCC2- 201224/495
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-QCC2- 201224/496
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

2 10 on(s): -	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	lletin/de cember- 2024- bulletin. html html https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-QCC7- 201224/497		
on(s): -	8.4	Configuring the SMR/S2CR register in Bypass mode.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	• •		
	8.4	Configuring the SMR/S2CR register in Bypass mode.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	• •		
02-Dec-2024	8.4	Configuring the SMR/S2CR register in Bypass mode.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	• •		
			bulletin. html			
02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCC7- 201224/498		
Product: qcf8000						
Affected Version(s): -						
)2-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-QCF8- 201224/499		
0	0 <mark>00</mark> n(s): -	0 00 n(s): -	2-Dec-20247.5beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063 000n(s): -Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which	2-Dec-2024 2-Dec-2024 2-Dec-2024 2-Dec-2024 2-Dec-2024 2-Dec-2024 2-Dec-2024 2-Dec-2024 2-Dec-2024 7.5 1 Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which 1 transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which 2-Dec-2024 7.5 1 transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which 1 transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which 1 transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which 1 transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which 1 transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qc	f 8001		CVE ID : CVE-2024-33063	urces/se curitybu lletin/de cember- 2024- bulletin. html	
Affected Ver					
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCF8- 201224/500
Product: qc	m2150			•	
Affected Ver	sion(s): -				
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCM2- 201224/501
Product: qc				1	I
Affected Ver	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCM4- 201224/502
Product: qc	m5430				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCM5- 201224/503
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCM5- 201224/504
Product: qc	m6490				
CVSSv3 Scoring		1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
*stands for all v	versions		Page 180 of 1127		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCM8- 201224/508
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCM8- 201224/509
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCM8- 201224/510
Product: qc					
Affected Vers	sion(s): -				

Integer Overflow or02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063H-QUA-QCN5- 201224/511Product: qcn62247.5Memory corruption while CONFID : CVE-2024-33063H-QUA-QCN5- 201224/511Affected Version(s): -VEID : CVE-2024-33063https:// docs.qua legith in htmlH-QUA-QCN6- 201224/511Improper Validation or (Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044H-QUA-QCN6- 201224/512Integer Overflow or wraparoun d02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info duct/pu bitresso cregister in Bypass mode. CVE ID : CVE-2024-33064H-QUA-QCN6- 201224/512Integer Wraparoun d02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info bitresso this element is present. CVE ID : CVE-2024-33063Https:// docs.qua lcomm.c om/pro duct/pu bitresso lcomm.c om/pro duct/pu bitresso length of the ML IE greater than the MI. IE inside which this element is present. CVE ID : CVE-2024-33063Https:// docs.qua lcomm.c om/pro duct/pu bitresso lcomm.c om/pro duct/pu bitresso length of the ML IE inside which this element is present. CVE ID : CVE-2024-33063Https:// docs.qua lcomm.c om/pro duct/pu bitresso lcomm.c om/pro duct/pu lettin/de cember- 2024- bulletin.	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu letin/de cember- 2024- builetin. httmsH-QUA-QCN6- 201224/512Integer Overflow or Wraparoun d02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063H-QUA-QCN6- 2024- builetin. httmsInteger Overflow or Wraparoun d02-Dec-20247.5Transient DOS while parsing the ML IE inside which this element is present. CVE ID : CVE-2024-33063H-QUA-QCN6- 2024- builetin. httmlProduct: quetzerTotal and the ML IE inside which this element is present. CVE ID : CVE-2024-33063H-QUA-QCN6- 2024- builetin. httml	Overflow or Wraparoun d		7.5	parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	• •
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso uritybu lletin/de cember- 2024- bulletin. httmlH-QUA-QCN6- 201224/512Integer Overflow or Wraparoun d02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063https:// docs.qua lcomm.c ources/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.cProduct: gcuezo2247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063H-QUA-QCN6- 2024- bulletin. htmlProduct: gcuezo234Tube parsing the ML IE when a beacon with common info length of the ML IE greater 						
Improper Validation of Array Index0.2-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044docs.qua icom.c ources/se urces/se urces/se Letin/de cember- 2024- bulletin. https:// docs.qua lcom.c om/pro duct/pu blicress urces/se icomsc- 2024- bulletin.H-QUA-QCN6- 201224/512Integer Overflow or Wraparoun d0.2-Dec-20247.5Fransient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063https:// docs.qua lcom.c om/pro duct/pu blicress urces/se urces/se urces/se urces/se urces/se urces/seProduct: cu-tu-tu-tu-tu-tu-tu-tu-tu-tu-tu-tu-tu-tu	Affected Vers	sion(s): -				
Integer Overflow or Wraparoun d02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de 2024- bulletin. htmlH-QUA-QCN6- 201224/513Product: qceb274	Validation of Array	02-Dec-2024	8.4	Configuring the SMR/S2CR register in Bypass mode.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	
	Overflow or Wraparoun	02-Dec-2024	7.5	parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	
CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Product: qc	n6274			1	
*stands for all versions			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	Affected Version(s): -						
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCN6- 201224/514		
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCN6- 201224/515		
Product: qc	n6402						
Affected Vers	sion(s): -						
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCN6- 201224/516		
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

n6412 sion(s): -							
sion(s): -							
	Affected Version(s): -						
02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCN6- 201224/517			
Product: qcn6422							
sion(s): -							
02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCN6- 201224/518			
n6432							
sion(s): -							
02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-QCN6- 201224/519			
	n6422 sion(s): - 02-Dec-2024 n6432 sion(s): -	n6422 sion(s): - 02-Dec-2024 7.5 n6432 sion(s): - 02-Dec-2024 7.5	02-Dec-20247.5Parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063m6422 sion(s): -Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-3306302-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063m6432Image: Common the multice is present is present. CVE ID : CVE-2024-3306302-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-3306302-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-3306302-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	02-Dec-20247.5Draming the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063Out/pu blicreso urces/se curitybu lletin.de cember- 2024- bulletin. httmln6422sion(s): -02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin.de cember- 2024- bulletin. httml02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin.de cember- 2024- bulletin. htmln64327.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin.de02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin.de02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
				cember- 2024- bulletin. html			
Product: qc	n7605			, 			
Affected Ver	sion(s): -						
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCN7- 201224/520		
Product: qc	Product: qcn7606						
Affected Ver	sion(s): -						
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCN7- 201224/521		
Product: qcn9000 Affected Version(s): -							
Integer Overflow or	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-QCN9- 201224/522		
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
Wraparoun d			than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qc					
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCN9- 201224/523
Product: qc	n9012				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCN9- 201224/524
Product: qc	n9024				l
Affected Ver	sion(s): -				

2-3

3-4

4-5

5-6

6-7

7-8

8-9

9-10

CVSSv3 Scoring Scale

*stands for all versions

0-1

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCN9- 201224/525
Product: qc					
Affected Ver	sion(s): -		Γ		
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCN9- 201224/526
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCN9- 201224/527

0-1

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

Use After Free02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua lcomm.c om/pro duct/pu blicreso curitybu lletin, de cember- 2024- builetin, htmlH-QUA-QCN9- 201224/528Buffer Over-read02-Dec-20246.1Information disclosure as invalid IPC message to NPU driver as the driver doesn't validate the IPC message to any ceritybu lletin, de cember- 2024- builetin, https:// docs.qua lcomm.c om/pro duct/pu blicreso treeso 2024- builetin, https:// docs.qua lcomm.c om/pro duct/pu blicreso letin, de cember- 2024- builetin, https:// docs.qua lcomm.c om/pro duct/pu blicreso letin, de cember- 2024- builetin, https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin, deProduct: qcn9160 Affected Version(s):-Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin, deBuffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c orduct/pu blicreso urces/se curitybu lletin, deProduct: qcn9274911-293344556677.889940	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read02-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-33037docs.qua lcommc. om/pro duct/pu blicreso 2024- builetin. htmlH-QUA-QCN9- 201224/529Product: qen9160Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// duct/pu blicreso urces/se curitybu letin/de cember- 2024- builetin. https:// duct/pu blicreso urces/se <br< td=""><td></td><td>02-Dec-2024</td><td>6.7</td><td>multiple threads try to unregister the CVP buffer at the same time.</td><td>docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.</td><td></td></br<>		02-Dec-2024	6.7	multiple threads try to unregister the CVP buffer at the same time.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	
Affected Version(s): - Affected Version(s): - Buffer Over-read 02-Dec-2024 8.4 Among		02-Dec-2024	6.1	NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	• •
Buffer Over-read02-Dec-20248.4Nemory corruption when allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlH-QUA-QCN9- 201224/530Product: qcruption when allocating and accessing an entry in an SMEM partition continuously.H-QUA-QCN9- 201224/530Product: gcruption when allocating and accessing an entry in an SMEM partition continuously.H-QUA-QCN9- 201224/530Product: gcruption when allocating and accessing an entry in an SMEM partition blicreso urces/se curitybu lletin. htmlH-QUA-QCN9- 201224/530Product: gcruption when allocating and accessing an entry in an SMEM partition continuously.H-QUA-QCN9- 201224/530Product: gcruption when allocating and accessing an entry in an SMEM partition blicreso urces/se curitybu lletin. htmlH-QUA-QCN9- 201224/530Product: gcruption when allocating and accessing an entry in an SMEM partition blicreso urces/se curitybu lletin. htmlProduct: gcruption when allocating and accessing an entry in an SMEM partition blicreso urces/se curitybu lletin. htmlProduct: gcruption when allocating and accessing an entry in an SMEM partition blicreso urces/se bulletin. htmlProduct: gcruption when allocating and accessing an entry in an SMEM partition blicreso urces/se curitybuProduct: gcruption when allocatin	Product: qc	n9160			1	
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlH-QUA-QCN9- 201224/530Product: qc-20248.48.4See 100000000000000000000000000000000000	Affected Ver	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	Over-read		8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	
5	Product: qc	n9274			•	
			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 Version(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCN9- 201224/531		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCN9- 201224/532		
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCN9- 201224/533		
Integer Overflow	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a	https:// docs.qua	H-QUA-QCN9- 201224/534		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparoun d			beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qc	s2290			I	
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS2- 201224/535
Product: qc	s410				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS4- 201224/536

CVSSv3 Scoring Scale0-11-22-33-44-5*stands for all versions

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS4- 201224/537
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS4- 201224/538
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS4- 201224/539
Buffer Over-read CVSSv3 Scoring	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-QCS4- 201224/540 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qc	s4290				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS4- 201224/541
Product: qc	s4490				
Affected Ver	sion(s): -			_	-
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS4- 201224/542
Product: qc				•	
Affected W	sion(s)·-				
Affected Ver	31011(3).				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS5- 201224/543
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS5- 201224/544
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS5- 201224/545
Product: qc				I	
Affected Vers	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS6- 201224/546
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS6- 201224/547
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS6- 201224/548
Use After Free CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-QCS6- 201224/549 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33053	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS6- 201224/550
Product: qc					
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS6- 201224/551
Product: qc					
Affected Ver	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS6- 201224/552
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS6- 201224/553
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS6- 201224/554
Integer Overflow or CVSSv3 Scoring	02-Dec-2024	7.5	Transient DOS whileparsing the ML IE when abeacon with common infolength of the ML IE greater-33-44-55-6	https:// docs.qua lcomm.c om/pro	H-QUA-QCS6- 201224/555 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparoun d			than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qc	s7230			I	
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS7- 201224/556
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS7- 201224/557
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-QCS7- 201224/558

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS7- 201224/559
s8155				
sion(s): -				
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS8- 201224/560
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-QCS8- 201224/561
	02-Dec-2024 s8155 sion(s): - 02-Dec-2024	Note Note Note	Image: Note of the series of	02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu letin/de cember- 2024- bulletin. httml02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httml02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httml

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qc	s8250				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS8- 201224/562
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS8- 201224/563
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-QCS8- 201224/564

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybu lletin/de cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS8- 201224/565
Product: qc	s8550				
Affected Vers	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS8- 201224/566
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-QCS8- 201224/567
CVSSv3 Scoring		1-2 2	- 3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Improper Improper Improper Overflow d02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052Ittps:// duct/pu Uletin/de combr- 2024- bulletin. https:// docs.qua leember- 2024- bulletin.Ittps:// duct/pu Uletin/de combr- 2024-43052Integer Overflow or Waparoun d02-Dec-20247.5Fransient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside while combre- 2024-33063Ittps:// docs.qua lecumetry bulletin. https:// docs.qua lecumetry bulletin. https:// docs.qua locametry bulletin. https:// docs.qua lecumetry bulletin. https:// docs.qua lecumetry bulketin.Ittps:// docs.qua locametry bulketin.Improper Validation lindex02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044Ittps:// docs.qua lecumetry bulketin.Improper Validation lindex02-Dec-20248.	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052docs.qua louct/pu blicreso urces/se urtiybu lletin/de cember- 2024- bulletin. htmlH-QUA-QCS8- 201224/568Integer Overflow or Wraparoun d02-Dec-20247.5Fransient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063H-QUA-QCS8- 20124/569Product: qcs9100Turproper Validation d02-Dec-20248.4Memory corruption while parsing the SMR/S2CR Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm. the symptoceH-QUA-QCS9- 20124/569Improper Validation Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR Configuring the SMR/S2CR ourtybuhttps:// docs.qua lcomm. torm. torm.https:// docs.qua lcomm. torm. torm.Improper Validation Index02-Dec-20248.4Memory corruption while configuring the SMR/S2CR configuring the SMR/S2CR ourtybuhttps:// docs.qua lcomm. torm. torm.Improper Validation Index02-Dec-20248.42344556677.88.99.00					cember- 2024- bulletin.	
Integer Overflow or Wraparoun d02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info 	Input	02-Dec-2024	7.8	processing API calls to NPU with invalid input.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	
Affected Version(s): - Improper Validation of Array Index 02-Dec-2024 8.4 Memory corruption while Configuring the SMR/S2CR register in Bypass mode. Dictores Undex VSSv3 Scoring Scale 0-1 1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Overflow or Wraparoun	02-Dec-2024	7.5	parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/deH-QUA-QCS9- 201224/570CVSSv3 Scoring Scale0-11-22-33-44-55-66-77-88-99-10	Product: qc	s9100				
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/deH-QUA-QCS9- 201224/570CVSSv3 Scoring Scale0-11-22-33-44-55-66-77-88-99-10	Affected Ver	sion(s): -				
	Validation of Array	02-Dec-2024	8.4	Configuring the SMR/S2CR register in Bypass mode.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	• •
			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
				cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QCS9- 201224/571
Product: qd					
Affected Ver	sion(s): -		Г	T	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QDU1- 201224/572
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-QDU1- 201224/573

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					
				2024- bulletin. html						
Product: qd	Product: qdu1010									
Affected Ver	Affected Version(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QDU1- 201224/574					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QDU1- 201224/575					
Product: qd	u1110				<u> </u>					
Affected Version(s): -										
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-QDU1- 201224/576					

CVSSv3 Scoring Scale0-11-22-33-44-5*stands for all versions

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QDU1- 201224/577
Product: qd	u1210				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QDU1- 201224/578
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-QDU1- 201224/579

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
				cember- 2024- bulletin. html						
Product: qd	Product: qdx1010									
Affected Ver	Affected Version(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QDX1- 201224/580					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QDX1- 201224/581					
Product: qd	x1011									
Affected Ver	Affected Version(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-QDX1- 201224/582					

Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curtybu lletin/de cember- 2024- bulletin. htmlH-QUA-QDX1- 2024- bulletin. l-QUA-QDX1- 2024- bulletin. htmlProduct: qep8111Memory corruption while continuously.https:// docs.qua lcomm.c ources/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/seH-QUA-QDX1- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/seH-QUA-QEP8- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/seH-QUA-QEP8- 201224/584Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056H-QUA-QEP8- 201224/584	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056docs.qua lcom.c om/pro duct/pu lletin/de cember- 2024- bulletin. htmlH-QUA-QDX1- 201224/583Product: qe>111Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33054https:// docs.qua lcom.re om/pro duct/pu blicreso urces/seH-QUA-QEP8- 2024- bulletin. https:// docs.qua lcom.re om/pro duct/pu blicreso urces/seH-QUA-QEP8- 2024- bulletin. https:// docs.qua lcom.re om/pro duct/pu blicreso urces/seH-QUA-QEP8- 2024- bulletin. https:// docs.qua lcom.re om/pro duct/pu blicreso urces/seH-QUA-QEP8- 2024- bulletin. https:// docs.qua lcom.re om/pro duct/pu blicreso urces/seH-QUA-QEP8- 2024- bulletin.Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33066https:// docs.qua lcom.re om/pro duct/pu blicreso urces/se					lletin/de cember- 2024- bulletin.	
Affected Version(s): -Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044 https:// docs.qua lcomm.c om/pro 		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044 https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se 201224/584Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056 https:// docs.qua letin/de cember- 2024- bulletin. htmlBuffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056 https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	Product: qe	p8111			I	
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044 docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlH-QUA-QEP8- 201224/584Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056 https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	Affected Vers	sion(s): -				
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.docs.qua lcomm.c om/pro duct/pu blicreso urces/seH-QUA-QEP8- 201224/585	Validation of Array	02-Dec-2024	8.4	Configuring the SMR/S2CR register in Bypass mode.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	
		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Product: qe	t4101				
Affected Ver	sion(s): -			T	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QET4- 201224/586
Product: qf					
Affected Ver	sion(s): -			T	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QFW7- 201224/587
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-QFW7- 201224/588

4-5

5-6

6-7

7-8

8-9

9-10

3-4

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QFW7- 201224/589
Product: qf	w7124				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QFW7- 201224/590
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-QFW7- 201224/591

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

		Description & CVE ID	Patch	NCIIPC ID
			curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QFW7- 201224/592
b5165m			I	I
sion(s): -				
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QRB5- 201224/593
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-QRB5- 201224/594
	b5165m sion(s): - 02-Dec-2024	b5165m sion(s): - 02-Dec-2024 8.4	02-Dec-20247.5parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063b5165m cve ID : CVE-2024-33063output output output output output output output output output output output output output output output output output outputMemory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-3304402-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	Image: Instant of the second

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Product: qr	b5165n				
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QRB5- 201224/595
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QRB5- 201224/596
Product: qr	u1032			I	I
Affected Ver	sion(s): -				-
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-QRU1- 201224/597

 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
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QRU1- 201224/598
Product: qr	u1052				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QRU1- 201224/599
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-QRU1- 201224/600

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
				curitybu lletin/de cember- 2024- bulletin. html	
Product: qr					
Affected Ver	sion(s): -		r		
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QRU1- 201224/601
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QRU1- 201224/602
Product: qs	m8250				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-QSM8- 201224/603

 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
				blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QSM8- 201224/604
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QSM8- 201224/605
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access.	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-QSM8- 201224/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33036	cember- 2024- bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QSM8- 201224/607
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QSM8- 201224/608
Product: qs					
Affected Ver	sion(s): -			https://	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-QSM8- 201224/609
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QSM8- 201224/610
Product: qs	w8573				
Affected Ver	sion(s): -				
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QSW8- 201224/611
Product: qt	s110				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-QTS1- 201224/612

CVSSv3 Scoring Scale0-11-22-33-44-55-66-77-8*stands for all versions

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Product: qx	m8083				
Affected Ver	sion(s): -			ſ	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-QXM8- 201224/613
	botics_rb3_pla	tform			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-ROBO- 201224/614
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-ROBO- 201224/615

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: ro	botics_rb5_pla	tform			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-ROBO- 201224/616
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-ROBO- 201224/617
Product: sa	2150p				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro	H-QUA-SA21- 201224/618
CVSSv3 Scoring		1-2 2	<mark>-3 3-4 4-5 5-6</mark>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: sa					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA41- 201224/619
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA41- 201224/620
Product: sa				I	
Allected ver	31011(3)				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA41- 201224/621
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA41- 201224/622
Product: sa	6145p			, 	
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA61- 201224/623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA61- 201224/624
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA61- 201224/625
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA61- 201224/626
Buffer Over-read CVSSv3 Scoring	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-SA61- 201224/627 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: sa					
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA61- 201224/628
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA61- 201224/629
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-SA61- 201224/630

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

2-Dec-2024	6.7	and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036 Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	
2-Dec-2024	6.7	multiple threads try to unregister the CVP buffer at	docs.qua lcomm.c om/pro duct/pu blicreso urces/se	
		CVE ID : CVE-2024-33053	curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA61- 201224/631
2-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA61- 201224/632
55		·		
on(s): -				
	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-SA61- 201224/633
r		ı(s): -	55 n(s): - 2-Dec-2024 8.4 Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	2024-bulletin. btml 55 1(s): - 2-Dec-2024 8.4 8.4 8.4 8.4 8.4 8.4 8.4 8.4 8.4 8.

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA61- 201224/634
Product: sa	6155p			·	
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA61- 201224/635
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-SA61- 201224/636

0-1

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

			curitybu	
			lletin/de cember- 2024- bulletin. html	
Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA61- 201224/637
Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA61- 201224/638
Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SA61- 201224/639
	Dec-2024	Dec-2024 6.7	Dec-20247.5parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063Dec-20246.7Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin.htmlDec-20247.5Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin.htmlDec-20246.7Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocation or invalid memory access. CVE ID : CVE-2024-33036https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin.htmlDec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua lcomm.c om/pro

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA61- 201224/640
Product: sa	<u> </u>				
Affected Ver	sion(s): -			I	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA72- 201224/641
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SA72- 201224/642

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA72- 201224/643
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA72- 201224/644
Product: sa	-				
Affected Ver	sion(s): -			latter - //	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SA77- 201224/645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA77- 201224/646
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA77- 201224/647
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA77- 201224/648
Product: sat	8145p			I	I
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 Version(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/649		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/650		
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/651		
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to	https:// docs.qua	H-QUA-SA81- 201224/652		

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/653
Product: sa	8150p				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/654
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https:// docs.qua lcomm.c	H-QUA-SA81- 201224/655
CVSSv3 Scoring *stands for all v		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
			entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/656
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/657
Buffer Over-read CVSSv3 Scoring	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware.	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-SA81- 201224/658 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33037	curitybu lletin/de cember- 2024- bulletin. html	
Product: sa					
Affected Ver	sion(s): -			I	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/659
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/660
Product: sa	8155p			L	
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-SA81- 201224/661

 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
				blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/662
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/663
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access.	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-SA81- 201224/664
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3 3-4 4-5 5-6</mark>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33036	cember- 2024- bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/665
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/666
Product: sa					
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-SA81- 201224/667
			-3 3-4 4-5 5-6		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/668
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/669
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/670

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
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/671
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA81- 201224/672
Product: sa	8255p				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA82- 201224/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA82- 201224/674
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA82- 201224/675
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA82- 201224/676
Use After Free CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-SA82- 201224/677 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: sa	8295p			I	
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA82- 201224/678
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA82- 201224/679
Integer Overflow or Wraparoun d CVSSv3 Scoring	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-SA82- 201224/680

			than the ML IE inside which	1.1.	
			than the ML TE Inside which this element is present. CVE ID : CVE-2024-33063	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA82- 201224/681
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA82- 201224/682
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-SA82- 201224/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
				cember- 2024- bulletin. html						
	Product: sa8530p									
Affected Ver	sion(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA85- 201224/684					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA85- 201224/685					
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-SA85- 201224/686					

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Free 02-Dec-2024 6.7 unregister the CVF bunker at the curry bunker at the same time. urces/se curritybu 201224/687 CVE ID : CVE-2024-33053 Illetin/de cember-2024-bulletin. bulletin. html html Buffer 02-Dec-2024 6.1 6.1 formation disclosure as NPU firmware can send invalid IPC message to NPU blicreso mrces (see H-QUA-SA85) H-QUA-SA85	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053docs.qua loc unces/se curitybu lletin/de cember- 2024- bulletin. htmlH-QUA-SA85 201224/687Buffer Over-read02-Dec-2024AAH-QUA-SA85 unces/se curitybu lletin/de cember- 2024- bulletin. htmlH-QUA-SA85 201224/687Buffer Over-read02-Dec-2024AAHH02-Dec-2024AAAAAAAAAABuffer Over-read02-Dec-2024AAAAOver-read02-Dec-2024AAAACVE ID : CVE-2024-33037AAAABuffer Over-read02-Dec-2024AAAACVE ID : CVE-2024-33037BAAABuffer Over-read02-Dec-2024AAAABuffer Over-read02-Dec-2024AAAABuffer Over-read02-Dec-2024AAAABuffer Over-read02-Dec-2024AAAABuffer Over-read02-Dec-2024AAAACVE ID : CVE-2024-33037BAAABuffer Over-readCCCAABuffer Over-readDCCBABuffer Over-readD					bulletin.	
Buffer Over-read02-Dec-20246.1Information disclosure as NPU firmware can send driver as the driver doesn't validate the IPC message received from the firmware.docs.qua Icomm.c om/pro duct/pu blicreso urces/se curitybu Iletin/deH-QUA-SA85 201224/688		02-Dec-2024	6.7	multiple threads try to unregister the CVP buffer at the same time.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	H-QUA-SA85- 201224/687
		02-Dec-2024	6.1	NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	H-QUA-SA85- 201224/688
Product: sa8540p	Product: sa	a8540p				
Affected Version(s): -	Affected Ver	ersion(s): -				
	Validation of Array	02-Dec-2024	8.4	Configuring the SMR/S2CR register in Bypass mode.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-SA85- 201224/689
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 versions			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
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA85- 201224/690
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA85- 201224/691
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA85- 201224/692

 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	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA85- 201224/693
Product: sa	-				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA86- 201224/694
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA86- 201224/695

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
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA86- 201224/696
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA86- 201224/697
Product: sa	8650p			•	
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA86- 201224/698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA86- 201224/699		
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA86- 201224/700		
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA86- 201224/701		
Product: sa8770p							
Affected Version(s): -							

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA87- 201224/702
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA87- 201224/703
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA87- 201224/704
Untrusted Pointer Dereferenc e CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the -3 3-4 4-5 5-6	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-SA87- 201224/705 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handle is not validated by the service. CVE ID : CVE-2024-33039	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: sa	8775p				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA87- 201224/706
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA87- 201224/707
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-SA87- 201224/708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA87- 201224/709
Product: sa					
Affected Ver	sion(s): -				[
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA90- 201224/710
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-SA90- 201224/711

			•		
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA90- 201224/712
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kerne and parsing which can lead to huge allocation or invalio memory access. CVE ID : CVE-2024-33036	curitybu	H-QUA-SA90- 201224/713
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-SA90- 201224/714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA90- 201224/715
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SA90- 201224/716
Product: sca	8180x				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SC81- 201224/717
CVSSv3 Scoring		1-2 2	<mark>-3 3-4 4-5 5-6</mark>	6-7 7-8	8-9 9-10
*stands for all v	versions		Page 250 of 1127		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SC81- 201224/718
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SC81- 201224/719
Product: sca					
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SC83- 201224/720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SC83- 201224/721
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SC83- 201224/722
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SC83- 201224/723

 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

Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// dccs.qua icomm.c om/pro duct/pu bilicreso urces/se curitybu lletin/de cember- 2024- bulletin. httmlImproper Restriction of Operations within the Bounds of a Memory02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053Https:// docs.qua icomm.c om/pro duct/pu bilicreso urces/se curitybu lletin/de cember- 2024- bulletin. httmlProduct: sd4607.8Memory corruption while information. CVE ID : CVE-2024-43053H-QUA-SC83- 201224/725Affected Version(s):-Toper 2024-43053Https:// docs.qua information. CVE ID : CVE-2024-33056Https:// docs.qua icomm.c om/pro duct/pu bilicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua icomm.c om/pro duct/pu bilicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua icomm.c om/pro duct/pu bilicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua icomm.c om/pro duct/pu bilicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua icomm.c om/pro duct/pu bilicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua icomm.c om/pro duct/pu bilicreso urces/se curitybu lletin/de cember- 2024- bulletin.P	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer0.2-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053docs.qua locmet. outc/pu bulletin. html letin/de cember- bulletin. htmlH-QUA-SC83- 0.01224/725Product: sduestarget diagnostic information. CVE ID : CVE-2024-43053H-QUA-SC83- curitybu letin/de cember- bulletin. htmlProduct: sduestarget diagnostic information. CVE ID : CVE-2024-33056https:// docs.qua letin/de cember- 2024/pu bulletin. https:// docs.qua letin/de cember- 2024/pu bulletin.Buffer Over-read0.2-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua letin/de cember- 2024- bulletin. htmlBuffer Over-read0.2-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua letin/de cember- 2024- bulletin. htmlProduct: sde/stargetstargetstargetstargetstargetBuffer0.2-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua bulletin. htmlProduct: sduestargetstargetstargetstargetstargetBuffer0.2-Dec-20248.4Starget	Input	02-Dec-2024	7.8	processing API calls to NPU with invalid input.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	e
Affected Version(s): -Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlhttps:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlProduct: storestorestore	Restriction of Operations within the Bounds of a Memory	02-Dec-2024	7.8	invoking IOCTL calls from user space to read WLAN target diagnostic information.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- builetin. htmlH-QUA-SD46- 201224/726Product: sd60	Product: sd	460		L		
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition CVE ID : CVE-2024-33056docs.qua lcomm.c oduct/pu blicreso urces/se Curitybu lletin/de cember- 2024- bulletin. htmlH-QUA-SD46- 201224/726Product: sdete	Affected Ver	sion(s): -				
	Over-read		8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•
CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Product: sd	660				
	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 Ver	sion(s): -	I			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD66- 201224/727
Product: sd	662				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD66- 201224/728
Product: sd	670			<u> </u>	
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-SD67- 201224/729

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

 *stands for all versions

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024- bulletin. html	
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD67- 201224/730
sion(s): -			T	
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD67- 201224/731
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SD67- 201224/732
	02-Dec-2024 02-Dec-2024	• •	Image: constraint of the symbol of the sym	Image: constraint of the system of the sys

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Product: sd	730				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD73- 201224/733
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD73- 201224/734
Product: sd	835				
Affected Ver	sion(s): -			-	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-SD83- 201224/735

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				cember- 2024- bulletin. html				
Product: sd	855							
Affected Ver	sion(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD85- 201224/736			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD85- 201224/737			
Product: sd865_5g								
Affected Version(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-SD86- 201224/738			

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

 *stands for all versions

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD86- 201224/739
02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD86- 201224/740
02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SD86- 201224/741
	02-Dec-2024	 марриализация и соверживания марриализация и	O2-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-3305602-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-4305202-Dec-20246.7Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access.	02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua letin/de cember- 2024- bulletin. html02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua letin/de cember- 2024- bulletin. html02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua letin/de cember- 2024- bulletin. html02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua letin/de cember- 2024- bulletin. html02-Dec-20246.7Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036https:// docs.qua ures/se curitybu licreso

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD86- 201224/742
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD86- 201224/743
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD86- 201224/744
Product: sd	888		I		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): -	I			
Improper Validation of Array Index	02-Dec-2024 8.4 Configuring the SMR/ register in Bypass mo		Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD88- 201224/745
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD88- 201224/746
Product: sd	m429w				
Affected Vers	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SDM4- 201224/747
CVSSv3 Scoring *stands for all v		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 Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SDM4- 201224/748
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SDM4- 201224/749
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SDM4- 201224/750
Stack- based Buffer Overflow CVSSv3 Scoring	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-SDM4- 201224/751 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			test command inside WLAN driver. CVE ID : CVE-2024-43050	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SDM4- 201224/752
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SDM4- 201224/753
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-SDM4- 201224/754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID						
				lletin/de cember- 2024- bulletin. html							
Product: sd	Product: sdx20m										
Affected Version(s): -											
Buffer Over-read 02-Dec-2024 8.4			Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SDX2- 201224/755						
Product: sd	x55										
Affected Ver	sion(s): -			1							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SDX5- 201224/756						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-SDX5- 201224/757						

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SDX5- 201224/758
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SDX5- 201224/759
Use of Out- of-range Pointer Offset CVSSv3 Scoring	02-Dec-2024 Scale 0-1	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-SDX5- 201224/760 8-9 9-10

Use After Free02-Dec-20246.7Memory corruption when multiple threads try to unregister the same time. CVE ID : CVE-2024-33053 https:// docs.qua letin/de camber- 2024- bulletin. httmlH-QUA-SDX5- 201224/761Buffer Over-read02-Dec-20246.1Information disclosure as invalid IPC message to NPU diver as the driver doesn' validate the IPC message to NPU driver as the driver doesn' validate the IPC message to NPU driver as the driver doesn' received from the firmware. CVE ID : CVE-2024-33037 H-QUA-SDX5- 201224/761Product: sdx57mInformation disclosure as neutripue received from the firmware. CVE ID : CVE-2024-33037H-QUA-SDX5- 201224/762Product: sdx57mMemory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urecrybe uletin/de cember- 2024- bulletin. html	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free0.2-Dec-20246.7Memory corruption when unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053docs.qua lout/pu bulicreso ucres/se ucres/se intes/nd docs.qua letin/de cember- 2024H-QUA-SDX5- 201224/761Buffer Over-read0.2-Dec-20246.1Information disclosure as NPU firmware can send invaild IPC message to NPU driver as the driver doesn't validate the IPC message to NPU driver as the driver doesn't urces/se UCE ID : CVE-2024-33037H-QUA-SDX5- 201224/762Freduct: storstorMemory corruption while driver as the driver doesn't validate the IPC message to NPU driver as the driver doesn't validate the IPC message to NPU letin/de cember- 2024- bulletin. httmH-QUA-SDX5- 201224/762Freduct: storstorMemory corruption while configuring the SMR/S2CR corribution driver as mode. CVE ID : CVE-2024-33044https:// docs.qua locs.qua					bulletin.	
Buffer Over-read02-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-33037docs.qua locumtybu blicreso uruelybu blicreso 2024- bulletin. htmlH-QUA-SDX5- 201224/762Product: state state state driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-33037docs.qua locometric docs.qua locos.qua loc		02-Dec-2024	6.7	multiple threads try to unregister the CVP buffer at the same time.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	
Affected Version(s): - https:// Improper 02-Dec-2024 8.4 Memory corruption while Configuring the SMR/S2CR om/pro Index 8.4 (D2-Dec-2024) 8.4 Memory corruption while Configuring the SMR/S2CR om/pro Undex Undex		02-Dec-2024	6.1	NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.chttps:// docs.qua lcomm.cH-QUA-SDX5- 201224/763Improper Validation of Array Index8.4Kemory corruption while Configuring the SMR/S2CR register in Bypass mode. UTEH-QUA-SDX5- 201224/763Improper Validation of Array Index8.4Kemory corruption while Configuring the SMR/S2CR register in Bypass mode. UTEH-QUA-SDX5- 201224/763Improper Validation Index8.4Kemory corruption while Configuring the SMR/S2CR register in Bypass mode. UTEH-QUA-SDX5- 201224/763Improper Validation Index8.4Kemory corruption while Configuring the SMR/S2CR register in Bypass mode. UTEH-QUA-SDX5- 201224/763Improper Validation Index8.4Kemory corruption while Configuring the SMR/S2CR register in Bypass mode. UTEH-QUA-SDX5- 201224/763Improper Validation Index1000000000000000000000000000000000000	Product: sd	x57m				
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-H-QUA-SDX5- 201224/763	Affected Ver	sion(s): -				
	Validation of Array	02-Dec-2024	8.4	Configuring the SMR/S2CR register in Bypass mode.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	-
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 * * 3-4 4-5 5-6 6-7 7-8 8-9 9-10			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
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SDX5- 201224/764
Product: sd	x61				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SDX6- 201224/765
Product: sd	x65m				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-SDX6- 201224/766

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID						
				cember- 2024- bulletin. html							
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SDX6- 201224/767						
Product: sd	Product: sdx71m										
Affected Ver	sion(s): -										
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056		H-QUA-SDX7- 201224/768						
Product: sd											
Affected Ver	sion(s): -										
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-SD_4- 201224/769						

 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				
				curitybu lletin/de cember- 2024- bulletin. html					
Product: sd_675									
Affected Ver	sion(s): -			Ι					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD_6- 201224/770				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD_6- 201224/771				
Product: sd	_8cx				· 				
Affected Ver	sion(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-SD_8- 201224/772				

 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
				blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD_8- 201224/773
Product: sd	_8_gen1_5g				
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SD_8- 201224/774
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-SD_8- 201224/775

Description & CVE ID		CV	Sv	CVSSv3	6v3	Description & CVE ID	Patch	NCIIPC ID
							urces/se curitybu lletin/de cember- 2024- bulletin. html	
cating a y in an tinuous		8.4		8.4		Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SG41- 201224/776
ilid inp oke GPU	7.8	7.8		7.8		Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SG41- 201224/777
cating a ry in an	8.4	8.4		8.4		Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro	H-QUA-SG82- 201224/778
		1-2			2	continuously.		om/pro

Weakness	Publish Date	CVSSv3	Descrip	otion & C	VE ID	Pa	tch	NCIII	PC ID
			CVE ID : CV	/E-2024	-33056	blic urce curi lleti cem 202	etin.		
Improper Input Validation	02-Dec-2024	7.8	Memory co processing with invalio CVE ID : CV	API call d input.	s to NPU	doc: lcom duct blic: urce curi lleti cem 202	t/pu reso es/se tybu n/de ber- 4- etin.	H-QUA- 201224	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063				s:// s.qua nm.c /pro t/pu reso es/se tybu n/de ber- 4- etin. 1	H-QUA- 201224	
Product: sm									
Affected Ver Buffer Over-read	02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.				os:// s.qua nm.c 'pro t/pu	H-QUA- 201224	
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			
			CVE ID : CVE-2024-33056	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html				
Product: sm								
Affected Vers	sion(s): -			1				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM46- 201224/782			
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM46- 201224/783			
Product: sm	Product: sm6250							
Affected Vers	sion(s): -							
Improper Validation	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode.	https:// docs.qua lcomm.c	H-QUA-SM62- 201224/784			
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 3-44-55-6	6-7 7-8	8-9 9-10			

of Array IndexCVE ID : CVE-2024-33044Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056Product: sm6250p	om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html https:// docs.qua lcomm.c	
Buffer Over-read02-Dec-20248.4allocating and accessing an entry in an SMEM partition continuously.CVE ID : CVE-2024-33056	docs.qua	
Product: sm6250p	om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM62- 201224/785
Affected Version(s): -	1	1
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM62- 201224/786
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.CVSSv3 Scoring Scale0-11-22-33-44-55-6	https://	H-QUA-SM62- 201224/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: sn	16370				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM63- 201224/788
Product: sn	17250p				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM72- 201224/789
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https:// docs.qua	H-QUA-SM72- 201224/790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM72- 201224/791
Product: sm Affected Ver					
Allected ver				https://	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	lictps:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM73- 201224/792
Buffer	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https:// docs.qua	H-QUA-SM73- 201224/793

Weakness Pu	ıblish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: sm732					
Affected Version	(s): -				
Improper Validation of Array Index	-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM73- 201224/794
Buffer Over-read 02-	-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM73- 201224/795
Product: sm855	50p				
Affected Version	(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM85- 201224/796
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM85- 201224/797
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM85- 201224/798
Integer Overflow or CVSSv3 Scoring	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-SM85- 201224/799 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparoun d			than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: sm	18635				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM86- 201224/800
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM86- 201224/801
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-SM86- 201224/802

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM86- 201224/803
Product: sm					
Affected Ver Buffer Over-read	sion(s): - 02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM87- 201224/804
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-SM87- 201224/805

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			urces/se curitybu lletin/de cember- 2024- bulletin. html				
02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM87- 201224/806			
02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM87- 201224/807			
Product: sm8750p							
sion(s): -			https://				
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-SM87- 201224/808			
	02-Dec-2024 02-Dec-2024 02-Dec-2024	• •	O2-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-4305202-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063R8750psion(s): -02-Dec-20248.402-Dec-20248.4	02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httml02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httml8750pMemory corruption when allocating and accessing an entry in an SMEM partitionhttps:// docs.qua lcomm.c om/pro			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybu lletin/de cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM87- 201224/809
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SM87- 201224/810
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SM87- 201224/811
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
				bulletin. html	
Product: sm	nart_audio_200	_platforn	n	·	
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SMAR- 201224/812
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SMAR- 201224/813
Product: sm	hart_audio_400	_platforn	n		
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-SMAR- 201224/814

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
				cember- 2024- bulletin. html		
Product: sna	apdragon_110	0_wearab	le_platform			
Affected Vers	sion(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/815	
Product: sna	apdragon_120	0_wearab	le_platform			
Affected Vers	sion(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/816	
Product: snapdragon_208_processor						
Affected Vers	sion(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-SNAP- 201224/817	
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-2024-33056	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/818
	apdragon_210	_processo)r		
Affected Ver Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/819
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-SNAP- 201224/820

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			
				urces/se curitybu lletin/de cember- 2024- bulletin. html				
Product: snapdragon_212_mobile_platform								
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/821			
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/822			
Product: snapdragon_425_mobile_platform								
Affected Ver	sion(s): -		Momony comunities while					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro	H-QUA-SNAP- 201224/823			
CVSSv3 Scoring *stands for all v		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
				duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: sn	apdragon_427	_mobile_p	olatform		
Affected Ver	sion(s): -				
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/824
Product: sn	apdragon_429	_mobile_p	olatform		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/825
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https:// docs.qua	H-QUA-SNAP- 201224/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/827
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/828
Stack- based Buffer Overflow CVSSv3 Scoring	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver.	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-SNAP- 201224/829 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-43050	urces/se curitybu lletin/de cember- 2024- bulletin. html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/830
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/831
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-SNAP- 201224/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
				2024- bulletin. html					
Product: snapdragon_430_mobile_platform									
Affected Ver	Affected Version(s): -								
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/833				
Product: sna	apdragon_435	_mobile_p	olatform						
Affected Ver	sion(s): -								
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/834				
Product: snapdragon_439_mobile_platform									
Affected Version(s): -									
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-SNAP- 201224/835				
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			
				urces/se curitybu lletin/de cember- 2024- bulletin. html				
Product: sn	apdragon_460	_mobile_p	olatform					
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/836			
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/837			
Product: snapdragon_480\+_5g_mobile_platform								
Affected Version(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro	H-QUA-SNAP- 201224/838			
CVSSv3 Scoring		1-2 2	<mark>-3 3-4 4-5 5-6</mark>	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/839
Product: sn	apdragon_480	_5g_mobi	le_platform	I	
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/840
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call.	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-SNAP- 201224/841

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Image: Burger of the second	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): - Affected Version(s): - Buffer Over-read 02-Dec-2024 8.4 Memory corruption when allocating and accessing an entry in an SMEM partition continuously. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html H-QUA-SNAP- 201224/842 Stack- based Buffer Overflow 02-Dec-2024 7.8 Memory corruption when invalid input is passed to invoke GPU Headroom API call. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html H-QUA-SNAP- 201224/843 Product: snaptragon_4 get_2 mobile_platform VE ID : CVE-2024-43048 https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html H-QUA-SNAP- 201224/843 Product: snaptragon_4 get_2 mobile_platform H-QUA-SNAP- 20224/844				CVE ID : CVE-2024-43048	urces/se curitybu lletin/de cember- 2024- bulletin.			
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu letin/de cember- 2024- bulletin. htmlH-QUA-SNAP- 201224/842Stack- based Buffer Overflow02-Dec-20247.8Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c oduct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c oduct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua letin/de cember- 2024- bulletin. https:// docs.qua letin/de curitybu lletin/de curity			en_1_mob	ile_platform				
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlH-QUA-SNAP- 201224/842Stack- based Buffer Overflow02-Dec-20247.8Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu letin/de cember- 2024- bulletin. https:// docs.qua hcurtybu letin/de cember- 2024- bulletin. https:// docs.qua hcurtybu letin/de cember- 2024- bulletin. https:// docs.qua hcurtybuFreduct: super-su	Affected Vers	sion(s): -			I			
Stack- based Buffer Overflow02-Dec-20247.8Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlH-QUA-SNAP- 201224/843Product: smart_agon_4_get_2_motionAffected Version(s): -Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an allocating and accessing anhttps:// docs.quaH-QUA-SNAP- 201224/844		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	-		
Affected Version(s): - Buffer 02-Dec-2024 8.4 Memory corruption when allocating and accessing an access	based Buffer	02-Dec-2024	7.8	invalid input is passed to invoke GPU Headroom API call.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	-		
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing anhttps:// docs.quaH-QUA-SNAP- 201224/844								
Over-read 02-Dec-2024 8.4 Memory corruption when allocating and accessing an docs.qua docs.qua 201224/844	Affected Version(s): -							
		02-Dec-2024	8.4		docs.qua			

 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
			entry in an SMEM partitie continuously. CVE ID : CVE-2024-330		om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
	apdragon_630	_mobile_p	olatform			
Affected Ver	sion(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing a entry in an SMEM partition continuously. CVE ID : CVE-2024-330	an on	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/845
Product: sn	apdragon_636	_mobile_p	olatform			
Affected Ver	sion(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing a entry in an SMEM partition continuously. CVE ID : CVE-2024-330	an on	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/846
Product: sn	apdragon_660	_mobile_p	olatform			1
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6	5-7 7-8	8-9 9-10
*stands for all v	versions		Dago 302 of 1127			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/847		
Product: sn	apdragon_662	_mobile_p	olatform				
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/848		
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/849		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Product: sn	Product: snapdragon_665_mobile_platform								
Affected Ver	sion(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/850				
	apdragon_670	_mobile_p	olatform						
Affected Ver	sion(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/851				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SNAP- 201224/852				

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					
				bulletin. html						
Product: sn	apdragon_675	_mobile_p	olatform							
Affected Ver	Affected Version(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/853					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/854					
Product: sn	apdragon_678	_mobile_p	olatform	I						
Affected Ver	sion(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-SNAP- 201224/855					

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				cember- 2024- bulletin. html				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/856			
Product: snapdragon_680_4g_mobile_platform								
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/857			
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-SNAP- 201224/858			

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
				2024- bulletin. html						
Product: sn	Product: snapdragon_685_4g_mobile_platform									
Affected Ver	sion(s): -									
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/859					
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/860					
Product: sn	apdragon_690	_5g_mobi	le_platform							
Affected Ver	Affected Version(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-SNAP- 201224/861					

2-3

3-4

4-5

5-6

6-7

7-8

8-9

9-10

0-1

Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056Hetin/de docs.qua letin/de cervipuHttps:// <docs.qua </docs.qua locomm.c om/pro duct/pu blicreso urces/se curritybu letin/de cervipuHttps:// <docs.qua </docs.qua letin/de cervipuHttps:// <docs.qua </docs.qua locomm.c ources/se curritybu letin/de cervipuHetures/se curritybu letin/de cervipuH-QUA-SNAP- 201224/862Use After Free02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua letin/de cervipuH-QUA-SNAP- 201224/863Use After Free02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua letin/de cervipuH-QUA-SNAP- 201224/863Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua letin/de cervipuBuffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua locomm locomm currybu lictin/de currybu lictin/de currybu lictin/de currybu lictin/dehttps:// docs.qua locomm locomm locomm locomm locomm locomm locomm locomm locomm locomm locomm locomm locomm locomm locomm	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an continuously. CVE ID : CVE-2024-33056docs.qua locm/pro duct/pu blicreso urces/se curitybuH-QUA-SNAP- 201224/862Use After Free02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33058https:// docs.qua loom/pro duct/pu blicreso ucres/seH-QUA-SNAP- 201224/863Use After Free02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua loom/pro duct/pu blicreso ucres/seH-QUA-SNAP- 201224/863Product: super-					cember- 2024- bulletin.	
Use After Free02-Dec-20246.76.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053docs.qua lcomm.c 		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•
Affected Version(s): -Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/deH-QUA-SNAP- 201224/864CVSSv3 Scoring Scale0-11-22-33-44-55-66-77-88-99-10		02-Dec-2024	6.7	multiple threads try to unregister the CVP buffer at the same time.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	e
Buffer Over-read 02-Dec-2024 8.4 Memory corruption when allocating and accessing an entry in an SMEM partition continuously. https:// docs.qua lcomm.c om/pro duct/pu blicreso H-QUA-SNAP- 201224/864 CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Product: sn	apdragon_695	_5g_mobi	le_platform		
Buffer Over-read 02-Dec-2024 8.4 Memory corruption when allocating and accessing an entry in an SMEM partition continuously. docs.qua lcom.c om/pro 	Affected Ver	sion(s): -				
		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	•
			1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
				cember- 2024- bulletin. html			
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/865		
Product: snapdragon_710_mobile_platform							
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/866		
	apdragon_712	_mobile_p	olatform				
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-SNAP- 201224/867		

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

 *stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
				curitybu lletin/de cember- 2024- bulletin. html						
	Product: snapdragon_720g_mobile_platform									
Affected Ver	sion(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/868					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/869					
	Product: snapdragon_730g_mobile_platform									
Affected Ver	sion(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-SNAP- 201224/870					

 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
				blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/871
	apdragon_730	_mobile_p	olatform		
Affected Ver	sion(s): -		L		ſ
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/872
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-SNAP- 201224/873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
				urces/se curitybu lletin/de cember- 2024- bulletin. html						
Product: sna	Product: snapdragon_732g_mobile_platform									
Affected Vers	sion(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/874					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/875					
	Product: snapdragon_750g_5g_mobile_platform									
Affected Vers	sion(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro	H-QUA-SNAP- 201224/876					
CVSSv3 Scoring *stands for all v		1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10					

Weakness	Publish Date	CVSSv3	Description & CV	'E ID	Patch	NCIIPC ID			
					duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption allocating and acces entry in an SMEM pa continuously. CVE ID : CVE-2024	sing an artition	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/877			
Use After Free	02-Dec-2024	6.7	Memory corruption multiple threads try unregister the CVP I the same time. CVE ID : CVE-2024	r to ouffer at	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/878			
	Product: snapdragon_765g_5g_mobile_platform								
Affected Ver	sion(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption Configuring the SMI register in Bypass m CVE ID : CVE-2024	R/S2CR node.	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-SNAP- 201224/879			
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 (5-7 7-8	8-9 9-10			

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/880			
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/881			
Product: snapdragon_765_5g_mobile_platform								
Affected Vers	sion(s): -			https://				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-SNAP- 201224/882			
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
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/883
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/884
	apdragon_768	g_5g_mob	ile_platform		
Affected Ver	sion(s): -		Γ		
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-SNAP- 201224/885
		1-2 2		blicreso	8-9

			curitybu	
			lletin/de cember- 2024- bulletin. html	
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/886
02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/887
	g\+_5g_m	obile_platform		
ion(s): -				
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-SNAP- 201224/888
j	02-Dec-2024 pdragon_778; ion(s): -	02-Dec-2024 6.7 pdragon_778g\+_5g_m ion(s): - 02-Dec-2024 8.4	02-Dec-20248.4allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-3305602-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053pdragon_778g\+_5g_mbile_platform ion(s): -CVE ID : CVE-2024-3305302-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056Icomm.c om/pro duct/pu lletin/de cember- 2024- bulletin. html02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se curitybupdragon_778g+_5g_motile_platform02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lletin/de cember- 2024- bulletin. html	
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/889
	g_5g_mob	oile_platform		
sion(s): -			https://	
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/890
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-SNAP- 201224/891
	02-Dec-2024 02-Dec-2024 02-Dec-2024	02-Dec-2024 8.4 apdragon_778 Jame 5g_mole sion(s): - 8.4	O2-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056apdragon_778g_sg_mobile_platformsion(s) : -02-Dec-20248.402-Dec-20248.402-Dec-20248.402-Dec-20248.402-Dec-20248.402-Dec-20248.4	02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httml02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Product: sn	apdragon_780	g_5g_mob	oile_platform		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/892
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/893
Product: sn	apdragon_782	g_mobile_	platform		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-SNAP- 201224/894

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

 *stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/895
Product: sna	apdragon_7c\+	-gen_3_c	ompute	I	
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/896
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-SNAP- 201224/897
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
				lletin/de cember- 2024- bulletin. html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/898
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/899
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SNAP- 201224/900

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Product: sn	apdragon_7c_c	ompute_j	platform		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/901
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/902
Product: sn	apdragon_7c_g	en_2_con	ipute_platform		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-SNAP- 201224/903

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/904
Product: sn	apdragon_820	automot	ive_platform		
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/905
-	apdragon_835	_mobile_p	oc_platform		
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-SNAP- 201224/906

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

 *stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				curitybu lletin/de cember- 2024- bulletin. html				
	apdragon_845	_mobile_p	olatform					
Affected Ver	sion(s): -			1				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/907			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/908			
Product: sn	Product: snapdragon_850_mobile_compute_platform							
Affected Ver	sion(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-SNAP- 201224/909			

 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

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/910
	\+			
sion(s): -				
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/911
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-SNAP- 201224/912
	02-Dec-2024 o2-Dec-2024 o2-Dec-2024	02-Dec-2024 8.4 apdragon_855 + sion(s): -	o2-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056apdragon_855\+sion(s): -02-Dec-20248.402-Dec-20248.402-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-3304402-Dec-20248.402-Dec-20248.4	02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin.de02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin.de cember- 2024- bulletin. html02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin.de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua locating and accessing an entry in an SMEM partition com/pro duct/pu02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition com/pro duct/pu

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
				urces/se curitybu lletin/de cember- 2024- bulletin. html			
Product: sna	apdragon_855	_mobile_p	olatform	1	I		
Affected Vers	sion(s): -						
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/913		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/914		
Product: snapdragon_860_mobile_platform							
Affected Vers	sion(s): -				ſ		
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro	H-QUA-SNAP- 201224/915		
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/916
Product: sn	apdragon_865	\+_5g_mo	bile_platform		
Affected Ver	sion(s): -			I	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/917
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-SNAP- 201224/918

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/919
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/920
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-SNAP- 201224/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/922
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/923
	apdragon_865	_5g_mobi	le_platform		
Affected Ver	sion(s): -			https://	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-SNAP- 201224/924
CVSSv3 Scoring *stands for all v		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
				2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/925
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/926
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/927

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
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/928
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/929
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/930
	apdragon_870	_5g_mobi	le_platform		
Affected Ver	sion(s): -				

0-1

1-2

2-3

5-6 6-7 8-9

9-10

7-8

*stands for all versions

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/931
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/932
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/933
Use of Out- of-range Pointer Offset CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-SNAP- 201224/934 8-9 9-10

*stands for all versions

Free02-Dec-20246.7race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040urces/se curitybu letin/de cember- 2024- bulletin. html201224/935Use After Free02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybuH-QUA-SNAF 201224/936Buffer Over-read02-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message received from the firmware.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybuH-QUA-SNAF 201224/936	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free02-Dec-20246.7Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040docs.qua loticreso urces/se curitybu lletin/de cember- 2024- bulletin. httmlH-QUA-SNAF 201224/935Use After Free02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httmlhttps:// docs.qua lcomm.c om/pro duct/pu blicreso letin/de cember- 2024- bulletin. httmlhttps:// docs.qua lcomm.c om/pro duct/pu blicreso letin/de cember- 2024- bulletin. httmlhttps:// docs.qua lcomm.c om/pro duct/pu blicreso urregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua lcomm.c om/pro duct/pu blicreso urres/se curitybu lletin/de cember- 2024- bulletin. htmlhttps:// docs.qua lcomm.c om/pro duct/pu lletin/de cember- 2024- bulletin. htmlhttps:// docs.qua lcomm.c om/pro duct/pu lletin/de cember- 2024- bulletin. htmlhttps:// docs.qua lcomm.c om/pro duct/pu locs.qua lcomm.c om/pro duct/pu lletin/de cember- 2024- bulletin. htmlhttps:// docs.qua lcomm.c om/pro duct/pu lletin/de lcomm.c om/pro duct/puBuffer Over-read02-Dec-20246.1Informa				and parsing which can lead to huge allocation or invalid memory access.	blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	
Use After Free02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlH-QUA-SNAF 201224/936Buffer Over-read02-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware.https:// docs.qua 		02-Dec-2024	6.7	invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	H-QUA-SNAP- 201224/935
Buffer Over-read02-Dec-20246.1NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware.docs.qua lcomm.c om/pro duct/puH-QUA-SNAF 201224/937		02-Dec-2024	6.7	multiple threads try to unregister the CVP buffer at the same time.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	H-QUA-SNAP- 201224/936
CVE ID : CVE-2024-33037 curitybu	Over-read			NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-SNAP- 201224/937 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
				lletin/de cember- 2024- bulletin. html			
Product: sn	apdragon_888	\+_5g_mo	bile_platform				
Affected Ver	sion(s): -			1			
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/938		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/939		
Product: sna	apdragon_888	_5g_mobi	le_platform	<u> </u>			
Affected Version(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-SNAP- 201224/940		

 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
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/941
	apdragon_8cx_	compute	_platform		
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/942
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-SNAP- 201224/943

			curitybu lletin/de cember- 2024- bulletin. html					
			11(1111					
02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/944				
Product: snapdragon_8cx_gen_2_5g_compute_platform								
sion(s): -								
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/945				
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-SNAP- 201224/946				
	pdragon_8cx_ ion(s): - 02-Dec-2024	pdragon_8cx_gen_2_5g ion(s): - 02-Dec-2024 8.4	test command inside wLAN driver. CVE ID : CVE-2024-43050pdragon_8cx_gen_2_5g_compute_platformion(s): -02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-3304402-Dec-20248.402-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	dest command inside wLAN driver. CVE ID : CVE-2024-43050curitybu lletin/de cember- 2024- bulletin. htmlpdragon_8cx_gen_2_5g_compute_platformhttps:// docs.qua lcomm.c om/pro duct/pu02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/947
		_gen_3_co	mpute_platform	•	
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/948
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-SNAP- 201224/949

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
				cember- 2024- bulletin. html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/950
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/951
	apdragon_8c_c	ompute_j	platform		
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-SNAP- 201224/952
CVSSv3 Scoring *stands for all v		1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/953
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/954
Product: sn	apdragon_8\+	_gen_1_m	obile_platform	I	
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SNAP- 201224/955
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3 3-4 4-5 5-6</mark>	6-7 7-8	8-9 9-10
stands for all v	rensions		Dage 270 of 1127		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
				bulletin. html						
Product: sn	Product: snapdragon_8\+_gen_2_mobile_platform									
Affected Ver	sion(s): -									
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/956					
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/957					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SNAP- 201224/958					

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/959
	apdragon_8_ge	en_1_mob	ile_platform	·	
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/960
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SNAP- 201224/961

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/962
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/963
	apdragon_8_ge	en_2_mob	ile_platform		
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SNAP- 201224/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/965
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/966
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/967
Product: sna	apdragon_8_ge	en_3_mob	ile_platform		
CVSSv3 Scoring		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 Ver	Affected Version(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/968			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/969			
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/970			

 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
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/971
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/972
Product: sna	apdragon_ar2_	gen_1_pla	atform		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/974
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/975
Product: sna	apdragon_auto	o_4g_mod	em		
Affected Ver	sion(s): -			-	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/977		
Product: sn	apdragon_auto	o_5g_mod	em-rf				
Affected Ver	sion(s): -						
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/978		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/979		
Product: snapdragon_auto_5g_modem-rf_gen_2							
CVSSv3 Scoring		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10		
*stands for all v	versions		Dage 227 of 1127				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Ver	sion(s): -						
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/980		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/981		
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/982		
Product: snapdragon_w5\+_gen_1_wearable_platform							
Affected Version(s): -							
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 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 Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/983
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/984
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/985
Use After Free CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-SNAP- 201224/986 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html				
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/987			
	apdragon_wea	r_1300_p	latform					
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/988			
	Product: snapdragon_wear_2100_platform							
Affected Ver	sion(s): -							

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/989
Product: sn	apdragon_wea	r_2500_p	latform	<u> </u>	
Affected Ver	sion(s): -				
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/990
	apdragon_wea	r_3100_p	latform		
Affected Ver	sion(s): -				
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SNAP- 201224/991

 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
				bulletin. html	
Product: sn	apdragon_wea	r_4100\+	_platform		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/992
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/993
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SNAP- 201224/994

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
				bulletin. html					
Product: sn	Product: snapdragon_x12_lte_modem								
Affected Ver	sion(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/995				
Product: sn	apdragon_x20	_lte_mode	em	1					
Affected Ver	sion(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/996				
	apdragon_x24	lte_mode	em						
Affected Ver	sion(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-SNAP- 201224/997				
CVSSv3 Scoring *stands for all v		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
				curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/998
Product: sna	apdragon_x35	_5g_mode	m-rf_system		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/999
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-SNAP- 201224/1000
CVSSv3 Scoring	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				lletin/de cember- 2024- bulletin. html				
Product: sn	apdragon_x50_	_5g_mode	em-rf_system					
Affected Ver	sion(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1001			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1002			
Product: sn	apdragon_x55	_5g_mode	em-rf_system	I				
Affected Version(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-SNAP- 201224/1003			

 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

			Description & CVE ID	Patch	NCIIPC ID
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1004
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1005
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-SNAP- 201224/1006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1007
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1008
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1009

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Product: sn	Product: snapdragon_x5_lte_modem								
Affected Ver	sion(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1010				
Product: sn	apdragon_x62	_5g_mode	em-rf_system						
Affected Ver	sion(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1011				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SNAP- 201224/1012				

4-5

5-6

6-7

7-8

8-9

9-10

3-4

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Product: sn	apdragon_x65	_5g_mode	em-rf_system		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1013
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1014
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SNAP- 201224/1015

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
				bulletin. html						
Product: sn	Product: snapdragon_x70_modem-rf_system									
Affected Ver	sion(s): -									
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1016					
Product: sn	apdragon_x72	_5g_mode	em-rf_system	1						
Affected Ver	sion(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1017					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-SNAP- 201224/1018					

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1019
	apdragon_x75	_5g_mode	em-rf_system	·	
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1020
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-SNAP- 201224/1021

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
				2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1022
Product: sna	apdragon_xr1_	platform			
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1023
Product: sn	apdragon_xr2	\+_gen_1_	platform		·
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-SNAP- 201224/1024

 CVSSv3 Scoring Scale
 0-1
 1-2
 2-3
 3-4

 *stands for all versions

4-5

5-6

6-7

7-8

8-9

Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056H-QUA-SNAP. 201224/1025Improper Input Validation02-Dec-20247.8Memory corruption while entry in an SMEM partition cortinuously. CVE ID : CVE-2024-33056H-QUA-SNAP. 201224/1025Improper Input Validation02-Dec-20247.8Memory corruption while entry in and the partition cortinuously. CVE ID : CVE-2024-33056H-QUA-SNAP. 201224/1025Improper Input Validation02-Dec-20247.8Memory corruption while entry in and the partition cortinuously. CVE ID : CVE-2024-43052H-QUA-SNAP. 201224/1026Improper Validation index02-Dec-20248.4Memory corruption while entry in and the partition com/pro duct/pu with invalid input. CVE ID : CVE-2024-43052H-QUA-SNAP. 201224/1026Improper Validation index02-Dec-20248.4Memory corruption while configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua locas, currybu licreso urces/se currybu licreso urces/se currybu licreso urces/se currybu licreso urces/se currybu licreso urces/se currybu licresoH-QUA-SNAP. 201224/1027	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read 0^2 -Dec-2024 8.4 $a^{Memory corruption whenallocating and accessing ancontinuously.CVE ID : CVE-2024-33056docs.qualocucres/seucres/$					cember- 2024- bulletin.	
Improper Input Validation of Array Index0.2-Dec-20247.87.8Memory corruption while processing API calls to NPU with invalid input. 		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	v
Affected Version(s): -Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/deH-QUA-SNAP- 201224/1027	Input	02-Dec-2024	7.8	processing API calls to NPU with invalid input.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•
Improper Validation of Array Index 02-Dec-2024 8.4 Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044 https:// docs.qua lcom.c om/pro blicreso urces/se curitybu lletin/de H-QUA-SNAP- 201224/1027	Product: sn	apdragon_xr2_	5g_platfo	rm		
Improper Validation of Array Index 02-Dec-2024 8.4 Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044 docs.qua lcom.c om/pro duct/pu blicreso urces/se curitybu lletin/de H-QUA-SNAP- 201224/1027	Affected Ver	sion(s): -				
	Validation of Array	02-Dec-2024	8.4	Configuring the SMR/S2CR register in Bypass mode.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	•
			1-2 2	<mark>-3 3-4 4-5 5-6</mark>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1028
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1029
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1031			
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1032			
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SNAP- 201224/1033			
	Product: srv1h							
Affected Ver	sion(s): -							

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SRV1- 201224/1034
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SRV1- 201224/1035
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SRV1- 201224/1036
Untrusted Pointer Dereferenc e CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the -3 3-4 4-5 5-6	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-SRV1- 201224/1037 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handle is not validated by the service. CVE ID : CVE-2024-33039	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: srv					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SRV1- 201224/1038
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SRV1- 201224/1039
Product: srv				I	
Affected Ver	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SRV1- 201224/1040
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SRV1- 201224/1041
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SRV1- 201224/1042
Untrusted Pointer Dereferenc e CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the -3 3-4 4-5 5-6	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-SRV1- 201224/1043 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handle is not validated by the service. CVE ID : CVE-2024-33039	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: ssg	g2115p				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SSG2- 201224/1044
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SSG2- 201224/1045
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https:// docs.qua lcomm.c om/pro duct/pu 6-7 7-8	H-QUA-SSG2- 201224/1046 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: ssg					
Affected Ver	sion(s): -		Γ		
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SSG2- 201224/1047
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SSG2- 201224/1048
Integer Overflow or Wraparoun d	02-Dec-2024 Scale 0-1	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-SSG2- 201224/1049 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33063	urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: sw	5100				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SW51- 201224/1050
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SW51- 201224/1051
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service.	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-SW51- 201224/1052

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		CVE ID : CVE-2024-33039	curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SW51- 201224/1053
02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SW51- 201224/1054
-				
sion(s): -				
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-SW51- 201224/1055
	02-Dec-2024 02-Dec-2024 02-Dec-2024	02-Dec-2024 6.7 02-Dec-2024 6.7 02-Dec-2024 6.1	O2-Dec-20246.7Wemory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-3304002-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-33037v5100pv5100pv3101v3102v3102v3103v3103v3104 <tr< td=""><td>O2-Dec-20246.7CVE ID : CVE-2024-33039curitybu lletin/de cember- 2024- bulletin. httm02-Dec-20246.7Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040https:// docs.qua lcomm.c. om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httm02-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-33037https:// docs.qua lcomm.c. om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httmv3-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro</td></tr<>	O2-Dec-20246.7CVE ID : CVE-2024-33039curitybu lletin/de cember- 2024- bulletin. httm02-Dec-20246.7Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040https:// docs.qua lcomm.c. om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httm02-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-33037https:// docs.qua lcomm.c. om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httmv3-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SW51- 201224/1056
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SW51- 201224/1057
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-SW51- 201224/1058

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
				bulletin. html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SW51- 201224/1059
Product: sx	r1120				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SXR1- 201224/1060
Product: sx	r1230p				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-SXR1- 201224/1061

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SXR1- 201224/1062
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SXR1- 201224/1063
Product: sxi					
Affected Ver	sion(s): -			http://	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-SXR2- 201224/1064
CVSSv3 Scoring *stands for all v		1-2 2	-3 3-44-55-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SXR2- 201224/1065
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SXR2- 201224/1066
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SXR2- 201224/1067

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SXR2- 201224/1068
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SXR2- 201224/1069
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SXR2- 201224/1070
Product: sxi	-				
Affected Ver	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SXR2- 201224/1071
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SXR2- 201224/1072
Product: sx	r2250p				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SXR2- 201224/1073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-SXR2- 201224/1074
Product: tal	ynplus				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-TALY- 201224/1075
	leo_collaborat	ion_vc1_p	olatform		
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-VIDE- 201224/1076

 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
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-VIDE- 201224/1077
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-VIDE- 201224/1078
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-VIDE- 201224/1079

 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	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-VIDE- 201224/1080
	leo_collaborat	ion_vc3_p	latform		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-VIDE- 201224/1081
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-VIDE- 201224/1082

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
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-VIDE- 201224/1083
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-VIDE- 201224/1084
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-VIDE- 201224/1085
Use After Free CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-VIDE- 201224/1086 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33053	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-VIDE- 201224/1087
Product: via	leo_collaborat	ion_vc5_p	latform		
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-VIDE- 201224/1088
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-VIDE- 201224/1089

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
		CVE ID : CVE-2024-33056	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html					
02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-VIDE- 201224/1090				
02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-VIDE- 201224/1091				
Product: vision_intelligence_300_platform								
sion(s): -			1					
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-VISI- 201224/1092				
	02-Dec-2024 02-Dec-2024	а а а а а а а а а а а а а а а а а а а	Image: CVE ID : CVE-2024-33056View	02-Dec-20247.8CVE ID : CVE-2024-33056 ources/se curitybu letin/de cember- 2024- bulletin. html02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu letin/de cember- 2024- bulletin. html02-Dec-20247.8Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater this element is present. CVE ID : CVE-2024-33063https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-2024- bulletin. html02-Dec-20248.4Memory corruption while parsing the ML IE when a beacon with common info length of the ML IE greater this element is present. CVE ID : CVE-2024-33063https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-2024- soluletin. html				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-VISI- 201224/1093
	sion_intelligen	ce_400_pl	atform		
Affected Ver	sion(s): -		1		
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-VISI- 201224/1094
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-VISI- 201224/1095

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-VISI- 201224/1096
02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-VISI- 201224/1097
cd9306				
sion(s): -				
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-WCD9- 201224/1098
	02-Dec-2024 02-Dec-2024 02-Dec-2024	02-Dec-2024 7.8 02-Dec-2024 7.5 02-Dec-2024 7.5	Image: Constraint of the systemImage: Constraint of the system02-Dec-20247.8Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-4304802-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063cd9306constraint of the systemo2-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	O2-Dec-2024A.B.Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httml02-Dec-20247.5Fransient DOS while parsing the ML IE when a beacon with common info length of the ML IE present. CVE ID : CVE-2024-33063https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin. httmld93065Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33066https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Product: wo	cd9326				
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1099
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1100
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-WCD9- 201224/1101

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Product: wo					
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1102
Product: wo	cd9335			<u> </u>	
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1103
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-WCD9- 201224/1104

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybu lletin/de cember- 2024- bulletin. html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1105
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1106
Product: wo					
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-WCD9- 201224/1107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1108
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1109
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-WCD9- 201224/1110

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Product: wo	cd9341				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1111
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1112
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-WCD9- 201224/1113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1114
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1115
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1116

0-1

1-2

2-3

Page **382** of **1137**

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1117
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1118
Product: wo	cd9360				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1120
Product: wo					
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1121
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1122

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1123
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1124
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1125
Integer Overflow or CVSSv3 Scoring	02-Dec-2024	7.5	Transient DOS whileparsing the ML IE when abeacon with common infolength of the ML IE greater-33-44-55-6	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-WCD9- 201224/1126 8-9 9-10

Weakness	Publish Date	CVSSv3	Description	n & CVE ID	Pat	tch	NCIII	PC ID
Wraparoun d			than the ML IE this element is CVE ID : CVE-2	present.	duct blicr urce curit lletin cem 2024 bulle html	eso s/se tybu n/de per- 4- etin.		
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corru parsing sensor camera driver, variable is use allocating men and parsing wi to huge allocat memory acces CVE ID : CVE-2	packets in user-space d while nory in kernel hich can lead ion or invalid s.	http: docs lcom duct blicr urce curit lletin cem 2024 bulle html	.qua im.c pro /pu eso s/se ybu h/de per- t- etin.	H-QUA- 201224	
Use After Free	02-Dec-2024	6.7	Memory corru multiple threa unregister the the same time. CVE ID : CVE-2	ds try to CVP buffer at	http: docs lcom om/ duct blicr urce curit lletin cem 2024 bulle html	.qua im.c pro /pu eso s/se ybu n/de per- t- etin.	H-QUA- 201224	
Buffer Over-read CVSSv3 Scoring	02-Dec-2024 Scale 0-1	6.1	Information di NPU firmware invalid IPC me driver as the d validate the IP received from CVE ID : CVE-2	can send ssage to NPU river doesn`t C message the firmware.	http: docs lcom om/ duct blicr urce curit	.qua im.c pro /pu eso s/se	H-QUA- 201224	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Product: wo	:d9371				
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1130
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1131
Product: wo	:d9375				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-WCD9- 201224/1132

 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

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			urces/se curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1133
02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1134
02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-WCD9- 201224/1135
	02-Dec-2024	 марриализация и соверхи и соверх	O2-Dec-20247.8Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-4304802-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-4305002-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-4305002-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input.	02-Dec-20247.8Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048urces/se curitybu letin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de02-Dec-20247.8Memory corruption while invoking API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de

Integer Overflow or wraparoun d02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the MI. IB greater than the MI. IE inside which this element is present. CVE ID : CVE-2024-33063https:// docs.gua locmm.c om/pro duct/pu blicreso urces/se curitybu length of the MI. IB greater table action with common info length of the MI. IB greater the selement is present. CVE ID : CVE-2024-33063H-QUA-WCD9- 201224/1136Use After Pree02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.gua lcomm.c om/pro duct/pu blicreso urces/se curitybu left.htmlH-QUA-WCD9- 201224/1136Preduct: wcd9378Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048https:// docs.gua lcomm.c om/pro duct/pu blicreso urces/se curitybu left.htmlStack- based Buffer OverflowStack- based Buffer Overflow02-Dec-20247.8Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048https:// docs.gua lcomm.c om/pro duct/pu blicreso urces/se curitybu lleth./de cember- 201224/1138	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparoun d02-Dec-20247.5Image: Second with common infole parsing the ML IE when a beacon with common infole length of the ML IE greater this element is present. CVE ID : CVE-2024-33063docs.qua curres/se curres/se 2024/1136H-QUA-WCD9- 01224/1136Use After Free02-Dec-20246.7AA					bulletin.	
Use After Free02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053docs qua lcomm.c om/pro duct/pu blicreso curitybu lletin/de cember- 2024- bulletin. htmlH-QUA-WCD9- 201224/1137Product: wcJ9378Memory corruption when invalid input is passed to invalid input is	Overflow or Wraparoun	02-Dec-2024	7.5	parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	-
Affected Version(s): - Affected Version(s): - Stack-based Nemory corruption when invalid input is passed to invoke GPU Headroom API call. https:// docs.qua lcomm.c Overflow 02-Dec-2024 7.8 Nemory corruption when invalid input is passed to invoke GPU Headroom API call. H-QUA-WCD9-201224/1138 CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10		02-Dec-2024	6.7	multiple threads try to unregister the CVP buffer at the same time.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•
Stack-based Buffer Overflow 02-Dec-2024 7.8 Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048 CUE ID : CVE-2024-43048 H-QUA-WCD9- blicreso urces/se Curitybu lletin/de c201224/1138 H-QUA-WCD9- blicreso 201224/1138 CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Product: wo	d9378				
Stack- based Buffer Overflow02-Dec-20247.8Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048docs.qua lcomm.c oduct/pu blicreso urces/se curitybu lletin/de cember- 2024-H-QUA-WCD9- 201224/1138CVSSv3 Scoring Scale0-11-22-33-44-55-66-77-88-99-10	Affected Ver	sion(s): -				
	based Buffer	02-Dec-2024	7.8	invalid input is passed to invoke GPU Headroom API call.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	-
			1-2 2	-3 3-44-55-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Product: wo	cd9380				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1139
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1140
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-WCD9- 201224/1141

3-4 4-5

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1142
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1143
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1144

 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
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1145
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1146
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1147
Use After Free CVSSv3 Scoring	02-Dec-2024 Scale 0-1	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-WCD9- 201224/1148 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33053	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1149
Product: wo	cd9385			L	
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1150
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call.	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-WCD9- 201224/1151

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID			tch	NCIII	PC ID
			CVE ID : CVE-	2024-43048	blicr urces curit lletir cemb 2024 bulle html	s/se ybu n/de oer- ŀ- etin.		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corru invoking IOCT user space to s private comm WLAN driver. CVE ID : CVE -2	L calls from set generic and inside	https docs lcom om/j duct, blicr urces curit lletir cem 2024 bulle html	.qua im.c pro /pu eso s/se ybu n/de per- t- etin.	H-QUA- 201224	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050			s:// .qua im.c pro /pu eso s/se ybu i/de per- t- etin.	H-QUA- 201224	
Improper Input Validation CVSSv3 Scoring	02-Dec-2024 Scale 0-1	7.8	Memory corru processing AP with invalid in CVE ID : CVE-	https docs lcom om/j duct, blicr urces curit lletir	.qua im.c pro /pu eso s/se s/se	H-QUA- 201224		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1155
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1156
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1157

Weakness	Publish Date	ublish Date CVSSv3 Description & CVE ID		Patch	NCIIPC ID				
Product: wo	cd9390	I							
Affected Ver	Affected Version(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1158				
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1159				
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1160				

Page **396** of **1137**

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1161
Product: wo					
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1162
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1163

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1164
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCD9- 201224/1165
Product: wcr	n3610			I	
Affected Vers	ion(s): -				
Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1166
Product: wcr	n3615			·	
CVSSv3 Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
sion(s): -	I			
02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1167
cn3620				
sion(s): -				
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1168
02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1169
	sion(s): - 02-Dec-2024 cm3620 sion(s): - 02-Dec-2024	sion(s): - 02-Dec-2024 7.8 02-Dec-2024 8.4 02-Dec-2024 7.8	sion(s): -Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052cm3620cm3620sion(s): -02-Dec-20248.48.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-3304402-Dec-20247.802-Dec-20247.8	sion(s): -Image: Si

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1170
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1171
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1172
Improper Restriction of Operations	02-Dec-2024 Scale 0-1	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-WCN3- 201224/1173 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			target diagnostic information. CVE ID : CVE-2024-43053	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1174
Product: wo	cn3660b				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1175
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call.	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-WCN3- 201224/1176

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID			Pat	tch	NCII	PC ID
			CVE ID : CVI	2-2024-430	48	blicr urce curit lletin cemi 2024 bulle html	s/se cybu n/de ber- 4- etin.		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory cor invoking IOC user space to private com WLAN drive CVE ID : CVI	TL calls from o set generic nand inside r.	m	http: docs lcom om/ duct blicr urce curit lletin cem 2024 bulle html	.qua im.c pro /pu eeso s/se sybu n/de ber- t- etin.	H-QUA- 201224	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050			http: docs lcom om/ duct blicr urce curit lletin cem 2024 bulle html	.qua im.c pro /pu eeso s/se sybu n/de ber- 4- etin.	H-QUA- 201224	
Improper Input Validation CVSSv3 Scoring	02-Dec-2024 Scale 0-1	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052			http: docs lcom om/ duct blicr urce curit lletin	.qua im.c pro /pu eso s/se cybu	H-QUA- 201224	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1180
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1181
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1183			
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1184			
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1185			
	Product: wcn3680							
Affected Ver	sion(s): -							

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1186
Product: wo					
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1187
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1188

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1189
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1190
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1191
Buffer Over-read CVSSv3 Scoring	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-WCN3- 201224/1192 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: wo	cn3950				
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1193
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1194
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-WCN3- 201224/1195

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1196
02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1197
sion(s): -			1	
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-WCN3- 201224/1198
	O2-Dec-2024 O2-Dec	o o	and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-3303602-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-3305302-Dec-20246.7Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-3303702-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode.	and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httml02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu02-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-33037https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro

Input Validation02-Dec-20247.8with invalid input. with invalid input. CVE ID : CVE-2024-43052urces/se curitybu lletin/de cember- 2024- bulletin. html201224/1199Use of Out- of-range Pointer Offset02-Dec-20246.7Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access.https:// docs.qua llcetin. https:// docs.qua lletin/de curitybu lletin/de curitybu lletin/deH-QUA-WCN3- 201224/1200Untrusted02-Dec-20246.7Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access.H-QUA-WCN3- 201224/1200Untrusted02-Dec-20246.7Memory corruption when and parsing which can lead to huge allocation or invalid memory access.https:// docs.qua lcomm.c om/pro	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052docs.qua lcom.c om/pro cember- 2024- bulletin.H-QUA-WCN3- 201224/1199Use of Out of-range Pointer Offset02-Dec-20246.7Memory corruption while parsing sensor packets in allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036https:// docs.qua letin.deHttps:// allocation or invalid blicreso urces/se curitybuUntrusted Pointer Dereference e02-Dec-20246.7Memory corruption while parsing sensor packets in allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036https:// docs.qua letin.deUntrusted Pointer Dereference e02-Dec-20246.7Memory corruption when parsing sensor packets in sensor packets in sensor packets in and parsing which can lead to huge allocation or invalid in htmlhttps:// docs.qua letin.deUntrusted Pointer Dereference e02-Dec-20246.7Memory corruption when passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33030https:// docs.qua location com/pro duct/pu blicreso urces/se urces/se					curitybu lletin/de cember- 2024- bulletin.	
Use of Out- of-range Pointer02-Dec-20246.7Memory corruption while parsing sensor packets in camera driver, user-space allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access.docs.qua lcomm.c om/pro duct/pu blicreso 	Input	02-Dec-2024	7.8	processing API calls to NPU with invalid input.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	H-QUA-WCN3- 201224/1199
Untrusted Pointer Dereferenc e02-Dec-20246.7Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service.docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/deH-QUA-WCN3- 201224/1201	of-range Pointer	02-Dec-2024	6.7	parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	-
	Pointer Dereferenc	02-Dec-2024	6.7	PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-WCN3- 201224/1201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1202
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1203
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1204

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Product: wo	Product: wcn3988								
Affected Ver	sion(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1205				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1206				
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1207				

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1208
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1209
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1210
Use After Free CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-WCN3- 201224/1211 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33053	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1212
Product: wo	cn3990			I	
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1213
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro duct/pu	H-QUA-WCN3- 201224/1214

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1215
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN3- 201224/1216
Product: wo					
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	H-QUA-WCN3- 201224/1217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				urces/se curitybu lletin/de cember- 2024- bulletin. html				
Product: wo	cn6740							
Affected Ver	sion(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN6- 201224/1218			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN6- 201224/1219			
Product: wcn6755								
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro	H-QUA-WCN6- 201224/1220			
CVSSv3 Scoring		1-2 2	<mark>-3</mark> 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-2024-33056	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN6- 201224/1221
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN6- 201224/1222
Integer Overflow or Wraparoun d	02-Dec-2024 Scale 0-1	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-WCN6- 201224/1223 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Product: wo	cn7860				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN7- 201224/1224
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN7- 201224/1225
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-WCN7- 201224/1226

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
				cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN7- 201224/1227
Product: wo	cn7861				
Affected Ver	sion(s): -			1	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN7- 201224/1228
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	H-QUA-WCN7- 201224/1229

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- bulletin. html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN7- 201224/1230
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN7- 201224/1231
Product: wo	n7880			I	
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-WCN7- 201224/1232
CVSSv3 Scoring		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10
*stands for all v	ersions		Page /10 of 1127		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN7- 201224/1233
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN7- 201224/1234
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN7- 201224/1235
Product: wo	m7881			1	
CVSSv3 Scoring *stands for all v		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 Ver	Affected Version(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN7- 201224/1236			
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN7- 201224/1237			
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WCN7- 201224/1238			
Integer Overflow	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a	https:// docs.qua	H-QUA-WCN7- 201224/1239			

0-1

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

		beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
a8810				L
sion(s): -				
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1240
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1241
02-Dec-2024	7.8	Memory corruption when invalid input is passed to	https:// docs.qua lcomm.c	H-QUA-WSA8- 201224/1242
	sion(s): - 02-Dec-2024 02-Dec-2024	sion(s): - 02-Dec-2024 8.4	this element is present. CVE ID : CVE-2024-33063a8810assion(s) : -02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-3304402-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-3305602-Dec-20247.8Memory corruption when	02-Dec-20248.4Memory corruption while CVE ID : CVE-2024-33063https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin. https:// docs.qua lcomm.c02-Dec-20248.4Memory corruption while configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin. httml02-Dec-20248.4Memory corruption while configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin. httml02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin. httml02-Dec-20247.8Memory corruption when anylid input is passed tohttps:// docs.qua

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			invoke GPU Headroom API call. CVE ID : CVE-2024-43048	om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1243
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1244
Use of Out- of-range Pointer Offset CVSSv3 Scoring	02-Dec-2024 Scale 0-1	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	H-QUA-WSA8- 201224/1245 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	curitybu lletin/de cember- 2024- bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1246
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1247
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-WSA8- 201224/1248
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
				bulletin. html	
Product: ws	sa8815				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1249
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1250
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-WSA8- 201224/1251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1252
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1253
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1254

Page **426** of **1137**

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1255		
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1256		
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1257		
	Product: wsa8830						
Affected Ver	sion(s): -						

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1258
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1259
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1260
Improper Restriction of Operations	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-WSA8- 201224/1261 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			private command inside WLAN driver. CVE ID : CVE-2024-43049	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1262
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1263
Integer Overflow or Wraparoun d	02-Dec-2024 Scale 0-1	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-WSA8- 201224/1264 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1265
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1266
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-WSA8- 201224/1267

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
				bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1268
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1269
Product: ws					
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-WSA8- 201224/1270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1271
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1272
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1273

 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
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1274
Product: ws					
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1275
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1276

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

					NCIIPC ID
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1277
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1278
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1279
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input.	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-WSA8- 201224/1280 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-43052	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1281
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1282
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-WSA8- 201224/1283 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1284
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1285
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-WSA8- 201224/1286

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Product: ws	sa8840				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1287
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1288
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	H-QUA-WSA8- 201224/1289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1290
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1291
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1292

 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
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1293
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1294
Product: ws	a8845			1	
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1296
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1297
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1298
Stack- based Buffer Overflow CVSSv3 Scoring	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory	https:// docs.qua lcomm.c om/pro 6-7 7-8	H-QUA-WSA8- 201224/1299 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			test command inside WLAN driver. CVE ID : CVE-2024-43050	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1300
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1301
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	H-QUA-WSA8- 201224/1302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Product: ws					
Affected Ver	sion(s): -		Г		
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1303
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1304
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	H-QUA-WSA8- 201224/1305

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
				cember- 2024- bulletin. html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1306
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1307
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1309
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	H-QUA-WSA8- 201224/1310
Vendor: toto	olink				
Product: ex	1800t				
Affected Vers	sion(s): -				
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Dec-2024	4.3	A vulnerability classified as problematic was found in TOTOLINK EX1800T 9.1.0cu.2112_B20220316. This vulnerability affects the function sub_40662C of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ssid leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed	N/A	H-TOT-EX18- 201224/1311
			· F · · · · · · · · · · · · · · ·		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
			to the public and may be used.							
			CVE ID : CVE-2024-12352							
Vendor: Tp-										
	Product: vn020_f3v									
Affected Vers	sion(s): -				1					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Dec-2024	6.5	A vulnerability classified as critical has been found in TP-Link VN020 F3v(T) TT_V6.2.1021. Affected is an unknown function of the file /control/WANIPConnection of the component SOAP Request Handler. The manipulation of the argument NewConnectionType leads to buffer overflow. The attack needs to be done within the local network. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12343		H-TPVN02- 201224/1312					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Dec-2024	6.3	A vulnerability, which was classified as critical, was found in TP-Link VN020 F3v(T) TT_V6.2.1021. This affects an unknown part of the component FTP USER Command Handler. The manipulation leads to memory corruption. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12344	N/A	H-TPVN02- 201224/1313					
	Operating System									
Vendor: App	ole									
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: ipa	ados		L	I	L
Affected Vers	sion(s): * Up to	(excluding	g) 17.7.3		
Access of Resource Using Incompatib le Type ('Type Confusion')	12-Dec-2024	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. CVE ID : CVE-2024-54505	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https://	O-APP-IPAD- 241224/1314
N/A	12-Dec-2024	7.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2,	https:// support. apple.co m/en-	O-APP-IPAD- 241224/1315
CVSSv3 Scoring	Scale 0-1	1-2 2	visionOS 2.2, tvOS 18.2,	us/1218 6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. CVE ID : CVE-2024-54479	37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 44, https://	
N/A	12-Dec-2024	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted font may result in	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https://	O-APP-IPAD- 241224/1316 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disclosure of process memory. CVE ID : CVE-2024-54486	support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42,	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	12-Dec-2024	5.9	A race condition was addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory mapping that can be written to. CVE ID : CVE-2024-54494	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co	O-APP-IPAD- 241224/1317 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43	
N/A	12-Dec-2024	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, macOS Ventura 13.7.2, iOS 18.1 and iPadOS 18.1, macOS Sonoma 14.7.2. Processing a malicious crafted file may lead to a denial-of-service. CVE ID : CVE-2024-44201	https:// support. apple.co m/en- us/1215 63, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 40,	O-APP-IPAD- 241224/1318
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2,	https:// support. apple.co m/en-	O-APP-IPAD- 241224/1319

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

VisionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 agle.co m/en- us/1218 agle.co m/en- us/1218 agle.co m/en- us/1218 agle.co m/en- us/1218 agle.co m/en- us/1218 agle.co m/en- us/1218 agle.co m/en- us/1218 agle.co m/en- us/1218 agle.co m/en- us/1218 agle.co m/en- us/1218 agle.co m/en- us/1218 agle.co m/en- us/1218 agle.co m/en- us/1218 agle.co m/en- us/1218 agle.co m/en- us/1218 agle.co m/en- us/1218 agle.co m/en- us/1218 add agle.co m/en- us/1218 agle.co m/en- us/1218 add agle.co m/en- us/1218 agle.co m/en- us/1218 add apple.co m/en- us/1218 add apple.co m/en- us/1218 add agle.co m/en- us/1218 add agle.co m/en- us/1218 add agle.co m/en- us/1218 add agle.co m/en- us/1218 add agle.co m/en- us/1218 add add agle.co m/en- us/1218 add add apple.co m/en- us/1218 add add agle.co m/en- us/1218 add add agle.co m/en- us/1218 add add apple.co m/en- us/1218 add a	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Execution using Shared Resource with12-Dec-20245.1addressed with improved locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOSsupport. apple.co m/en- us/1218o-APP-IPAD- 241224/1320Improper Synchroniz ation ('Race Condition')5.1Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS0-APP-IPAD- 241224/1320				macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory.	37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218	
	Execution using Shared Resource with Improper Synchroniz ation ('Race	12-Dec-2024	5.1	addressed with improved locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to leak sensitive	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-54510	https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42,	
N/A	sion(s): * Up to 12-Dec-2024	9.8	The issue was addressed with improved bounds checks. This issue is fixed in iOS 18.1 and iPadOS 18.1. An attacker may be able to cause unexpected system termination or arbitrary code execution in DCP firmware. CVE ID : CVE-2024-44299	https:// support. apple.co m/en- us/1215 63	O-APP-IPAD- 241224/1321
Origin Validation Error	12-Dec-2024	5.3	A cookie management issue was addressed with improved state management. This issue is fixed in Safari 18.1, visionOS 2.1, tvOS 18.1, iOS 18.1 and iPadOS 18.1, watchOS 11.1. Cookies belonging to one	https:// support. apple.co m/en- us/1215 63, https:// support.	O-APP-IPAD- 241224/1322
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
			origin may be sent to another origin. CVE ID : CVE-2024-44212	apple.co m/en- us/1215 65, https:// support. apple.co m/en- us/1215 66, https:// support. apple.co m/en- us/1215 69, https:// support. apple.co m/en- us/1215 71	
N/A	12-Dec-2024	3.3	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 18.1 and iPadOS 18.1. An app may be able to read sensitive location information. CVE ID : CVE-2024-44200	https:// support. apple.co m/en- us/1215 63	O-APP-IPAD- 241224/1323
N/A	12-Dec-2024	3.3	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 18.1 and iPadOS 18.1, watchOS 11.1. An app may be able to determine a user's current location. CVE ID : CVE-2024-44290	https:// support. apple.co m/en- us/1215 63, https:// support. apple.co m/en- us/1215 65	O-APP-IPAD- 241224/1324

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 Version(s): * Up to (excluding) 18.2								
Out-of- bounds Write	12-Dec-2024	9.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. CVE ID : CVE-2024-54534	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 45, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 45, https://	0-APP-IPAD- 241224/1325			
N/A	12-Dec-2024	7.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2,	https:// support. apple.co m/en- us/1218 37,	O-APP-IPAD- 241224/1326			

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. CVE ID : CVE-2024-54508	https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 45, https:// support. apple.co m/en- us/1218 45, https:// support. apple.co m/en- us/1218 45, https://	
N/A	12-Dec-2024	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2. An app may be able to access sensitive user data.	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218	O-APP-IPAD- 241224/1327
			CVE ID : CVE-2024-54513	39, https:// support.	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 45	
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious app may be able to access private information. CVE ID : CVE-2024-54526	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co	O-APP-IPAD- 241224/1328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/1218 43, https:// support. apple.co m/en- us/1218 44 https://	
N/A	12-Dec-2024	5.5	This issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access sensitive user data. CVE ID : CVE-2024-54527	support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218	O-APP-IPAD- 241224/1329

4-5 3-4

5-6

8-9

9-10

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/1218 44	
N/A	12-Dec-2024	4.2	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in iOS 18.2 and iPadOS 18.2. Muting a call while ringing may not result in mute being enabled.	https:// support. apple.co m/en- us/1218 37	O-APP-IPAD- 241224/1330
Affected Ver	cion(c); * Un to	(including	CVE ID : CVE-2024-54503		
Anected ver	sion(s): * Up to	enciuaing	5J 1/./.J	http://	
N/A	12-Dec-2024	2.4	The issue was addressed by adding additional logic. This issue is fixed in iPadOS 17.7.3, iOS 18.2 and iPadOS 18.2. An attacker with physical access to an iOS device may be able to view notification content from the lock screen. CVE ID : CVE-2024-54485	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38	O-APP-IPAD- 241224/1331
Affected Ver	<mark>sion(s): From (</mark> i	ncluding)	18.0 Up to (excluding) 18.1		
N/A	12-Dec-2024	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, macOS Ventura 13.7.2, iOS 18.1 and iPadOS 18.1, macOS Sonoma 14.7.2. Processing a malicious crafted file may lead to a denial-of-service. CVE ID : CVE-2024-44201	https:// support. apple.co m/en- us/1215 63, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218	O-APP-IPAD- 241224/1332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): From (i	ncluding)	18.0 Up to (excluding) 18.2	40, https:// support. apple.co m/en- us/1218 42	
Access of Resource Using Incompatib le Type ('Type Confusion')	12-Dec-2024	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. CVE ID : CVE-2024-54505	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218	O-APP-IPAD- 241224/1333

0-1

1-2

3-4 4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/1218 45	
N/A	12-Dec-2024	7.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. CVE ID : CVE-2024-54479	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https://	O-APP-IPAD- 241224/1334
N/A	12-Dec-2024	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2,	https:// support. apple.co m/en- us/1218	O-APP-IPAD- 241224/1335

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted font may result in the disclosure of process memory. CVE ID : CVE-2024-54486	37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	12-Dec-2024	5.9	A race condition was addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https://	O-APP-IPAD- 241224/1336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mapping that can be written to. CVE ID : CVE-2024-54494	support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co	
N/A CVSSv3 Scoring	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory. CVE ID : CVE-2024-54500	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co	O-APP-IPAD- 241224/1337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	12-Dec-2024	5.1	A race condition was addressed with improved locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to leak sensitive kernel state. CVE ID : CVE-2024-54510	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218	0-APP-IPAD- 241224/1338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				42, https:// support. apple.co m/en- us/1218 43	
N/A	12-Dec-2024	2.4	The issue was addressed by adding additional logic. This issue is fixed in iPadOS 17.7.3, iOS 18.2 and iPadOS 18.2. An attacker with physical access to an iOS device may be able to view notification content from the lock screen. CVE ID : CVE-2024-54485	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38	O-APP-IPAD- 241224/1339
Product: ipl	none_os				
Affected Ver	sion(s): * Up to	(excluding	g) 18.1		
N/A	12-Dec-2024	9.8	The issue was addressed with improved bounds checks. This issue is fixed in iOS 18.1 and iPadOS 18.1. An attacker may be able to cause unexpected system termination or arbitrary code execution in DCP firmware. CVE ID : CVE-2024-44299	https:// support. apple.co m/en- us/1215 63	O-APP-IPHO- 241224/1340
N/A	12-Dec-2024	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, macOS Ventura 13.7.2, iOS 18.1 and iPadOS 18.1, macOS Sonoma 14.7.2. Processing a malicious crafted file may lead to a denial-of-service. CVE ID : CVE-2024-44201	https:// support. apple.co m/en- us/1215 63, https:// support. apple.co m/en- us/1218	O-APP-IPHO- 241224/1341
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
				38, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	
Origin Validation Error	12-Dec-2024	5.3	A cookie management issue was addressed with improved state management. This issue is fixed in Safari 18.1, visionOS 2.1, tvOS 18.1, iOS 18.1 and iPadOS 18.1, watchOS 11.1. Cookies belonging to one origin may be sent to another origin. CVE ID : CVE-2024-44212	https:// support. apple.co m/en- us/1215 63, https:// support. apple.co m/en- us/1215 65, https:// support. apple.co m/en- us/1215 66, https:// support. apple.co m/en- us/1215 66, https:// support. apple.co m/en- us/1215 71	O-APP-IPHO- 241224/1342

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
N/A	12-Dec-2024	3.3	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 18.1 and iPadOS 18.1. An app may be able to read sensitive location information. CVE ID : CVE-2024-44200	https:// support. apple.co m/en- us/1215 63	O-APP-IPHO- 241224/1343
N/A	12-Dec-2024	3.3	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 18.1 and iPadOS 18.1, watchOS 11.1. An app may be able to determine a user's current location. CVE ID : CVE-2024-44290	https:// support. apple.co m/en- us/1215 63, https:// support. apple.co m/en- us/1215 65	O-APP-IPHO- 241224/1344
Affected Ver	sion(s): * Up to	(excluding	g) 18.2		
Out-of- bounds Write	12-Dec-2024	9.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. CVE ID : CVE-2024-54534	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en-	O-APP-IPHO- 241224/1345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/1218 44, https:// support. apple.co m/en- us/1218 45, https:// support. apple.co m/en- us/1218 46	
Access of Resource Using Incompatib le Type ('Type Confusion')	12-Dec-2024	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. CVE ID : CVE-2024-54505	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44,	O-APP-IPHO- 241224/1346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https:// support. apple.co m/en- us/1218 45 https://	
N/A	12-Dec-2024	7.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. CVE ID : CVE-2024-54479	support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co	O-APP-IPHO- 241224/1347

4-5 3-4

5-6

6-7

8-9

9-10

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2024	7.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. CVE ID : CVE-2024-54508	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 45, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co	0-APP-IPH0- 241224/1348
N/A	12-Dec-2024	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2,	https:// support. apple.co m/en- us/1218 37, https:// support.	O-APP-IPHO- 241224/1349
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
			macOS Sonoma 14.7.2. Processing a maliciously crafted font may result in the disclosure of process memory. CVE ID : CVE-2024-54486	apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42,	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	12-Dec-2024	5.9	A race condition was addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory mapping that can be written to. CVE ID : CVE-2024-54494	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en-	0-APP-IPHO- 241224/1350 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43	
N/A CVSSv3 Scoring	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory. CVE ID : CVE-2024-54500	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218	0-APP-IPH0- 241224/1351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43	
N/A	12-Dec-2024	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2. An app may be able to access sensitive user data. CVE ID : CVE-2024-54513	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co	O-APP-IPHO- 241224/1352

4-5 3-4

5-6

8-9

9-10

0-1

1-2

Weakness	Publish Date	CVSSv3	Descripti	Pa	atch	NCIIP	CID	
N/A	12-Dec-2024	5.5	issue is fixed 11.2, tvOS 18 Sequoia 15.2 iPadOS 18.2, Ventura 13.7 Sonoma 14.7 app may be a private inform	ed checks. Thi in watchOS .2, macOS , iOS 18.2 and macOS .2, macOS .2. A maliciou ble to access	s sup app m/d us/ 37, http sup app m/d us/ 39, http sup app m/d us/ 40, http sup app m/d us/ 40, http sup app m/d us/ 40, http sup app m/d us/ 39, http sup app m/d us/ 39, http sup app m/d us/ 39, http sup m/d us/ 39, http sup m/d us/ 39, http sup m/d us/ 39, http sup m/d us/ 39, http sup m/d us/ 40, http sup sup m/d us/ 40, http sup sup m/d us/ 40, http sup sup sup m/d sup sup m/d sup sup sup sup sup sup sup sup sup sup	1218 pos:// port.	0-APP-I 241224	
N/A	12-Dec-2024	5.5	issue is fixed 11.2, tvOS 18 Sequoia 15.2 iPadOS 18.2, Ventura 13.7	ed checks. Thi in watchOS .2, macOS , iOS 18.2 and macOS	s sup app m/o us/ 37, http	os:// port. ole.co en- 1218 os:// port.	O-APP-I 241224	
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
			be able to access sensitive user data. CVE ID : CVE-2024-54527	apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43,	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	12-Dec-2024	5.1	A race condition was addressed with improved locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to leak sensitive kernel state. CVE ID : CVE-2024-54510	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- 6-7 7-8	O-APP-IPHO- 241224/1355

Weakness	Publish Date	CVSSv3		Descri	ption & C	CVE ID		Pat	tch	NCIIPC ID		
								us/1 39, http: supp appl m/ei us/1 40, http: supp us/1 42, http: supp appl m/ei us/1 43	s:// oort. e.co n- 218 s:// oort. e.co n- 218 s:// oort. e.co n-			
N/A	12-Dec-2024	4.2	inta ada sta issu iPa wh in u	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in iOS 18.2 and iPadOS 18.2. Muting a call while ringing may not result in mute being enabled.				http: supp appl m/e: us/1 37	oort. e.co n-	O-APP- 241224		
N/A	12-Dec-2024	2.4	add iss 17. 18. phy dev not the	CVE ID : CVE-2024-54503 The issue was addressed by adding additional logic. This issue is fixed in iPadOS 17.7.3, iOS 18.2 and iPadOS 18.2. An attacker with physical access to an iOS device may be able to view notification content from the lock screen. CVE ID : CVE-2024-54485				http: supp appl m/ei us/1 37, http: supp appl m/ei us/1 38	oort. e.co 218 s:// oort. e.co n-	O-APP- 241224		
Product: ma	acos		•				·					
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): -	1			
Integer Underflow (Wrap or Wraparoun d)	10-Dec-2024	 Bridge versions 14.1.3, 15.0 and earlier are affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2024-53955 		https:// helpx.ad obe.com /securit y/produ cts/brid ge/apsb 24- 103.htm l	O-APP-MACO- 241224/1358
Heap- based Buffer Overflow	10-Dec-2024	7.8	Premiere Pro versions 25.0, 24.6.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2024-53956	https:// helpx.ad obe.com /securit y/produ cts/pre miere_p ro/apsb 24- 104.htm l	O-APP-MACO- 241224/1359
Affected Vers	sion(s): * Up to	(excluding	g) 13.7.2		L
Affected Version(s): * Up to (exclusion)N/A12-Dec-20248.8		8.8	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to break out of its sandbox. CVE ID : CVE-2024-54498	https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support.	O-APP-MACO- 241224/1360
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 <mark>9-1</mark> 0

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.co m/en- us/1218 42	
N/A	12-Dec-2024	7.8	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Running a mount command may unexpectedly execute arbitrary code. CVE ID : CVE-2024-54489	https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	O-APP-MACO- 241224/1361
N/A	12-Dec-2024	7.1	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to overwrite arbitrary files. CVE ID : CVE-2024-54528	https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	O-APP-MACO- 241224/1362
N/A	12-Dec-2024	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS	https:// support. apple.co	O-APP-MACO- 241224/1363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted font may result in the disclosure of process memory. CVE ID : CVE-2024-54486	m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42, https://	
Concurrent Execution using Shared Resource with Improper Synchroniz ation	12-Dec-2024	5.9	A race condition was addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218	O-APP-MACO- 241224/1364
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
('Race Condition')			mapping that can be written to. CVE ID : CVE-2024-54494	38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43	
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access user- sensitive data. CVE ID : CVE-2024-54474	https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	O-APP-MACO- 241224/1365

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
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access user- sensitive data. CVE ID : CVE-2024-54477	https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	O-APP-MACO- 241224/1366
N/A CVSSv3 Scoring	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory. CVE ID : CVE-2024-54500	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co	0-APP-MACO- 241224/1367

	1				
				apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43	
N/A	12-Dec-2024	5.5	This issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access sensitive user data. CVE ID : CVE-2024-54527	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en-	O-APP-MACO- 241224/1368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/1218 44	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	12-Dec-2024	5.1	A race condition was addressed with improved locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to leak sensitive kernel state. CVE ID : CVE-2024-54510	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co	O-APP-MACO- 241224/1369
Affected Ver	sion(s): * Up to	(excluding	g) 15.2		
N/A	12-Dec-2024	9.8	A logic issue was addressed with improved state management. This issue is fixed in macOS Sequoia	https:// support. apple.co m/en-	O-APP-MACO- 241224/1370
CVSSv3 Scoring *stands for all v		1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

bounds Read 12-Dec-2024 9.8 Inay be able to cause unexpected system termination or arbitrary code execution in DCP firmware. m/en- us/1218 39 241224/1371 CVE ID : CVE-2024-54506 https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co Out-of- bounds 12-Dec-2024 9.8 Sequoia 15-2, Safari 18.2, Sequoia 15-2, Safari 18.2, 0-APP-MACO	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read12-Dec-20249.8An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.2. An attacker may be able to cause unexpected system termination or arbitrary code execution in DCP firmware.https:// support. aple.co m/en- us/1218 39o-APP-MACO 241224/1371Out-of- bounds12-Dec-20249.8The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption.https:// support. aple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support.						
Out-of- bounds Read12-Dec-20249.8issue was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.2. An attacker may be able to cause unexpected system termination or arbitrary code execution in DCP firmware. CVE ID : CVE-2024-54506https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 43, https:// support.0.APP-MACO 241224/1372 us/218 44, https:// support.				CVE ID : CVE-2024-54465		
Out-of- bounds12-Dec-20249.8The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption.0-APP-MACO apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support.	bounds	12-Dec-2024	9.8	issue was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.2. An attacker may be able to cause unexpected system termination or arbitrary code execution in DCP firmware.	support. apple.co m/en- us/1218	O-APP-MACO- 241224/1371
m/en- us/1218	bounds	12-Dec-2024	9.8	with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption.	support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en-	O-APP-MACO- 241224/1372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				45, https:// support. apple.co m/en- us/1218 46	
Access of Resource Using Incompatib le Type ('Type Confusion')	12-Dec-2024	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. CVE ID : CVE-2024-54505	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co	O-APP-MACO- 241224/1373
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 3-44-555-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2024	7.8	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sequoia 15.2. A malicious app may be able to gain root privileges. CVE ID : CVE-2024-54515	https:// support. apple.co m/en- us/1218 39	O-APP-MACO- 241224/1374
N/A	12-Dec-2024	7.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. CVE ID : CVE-2024-54479	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https://	O-APP-MACO- 241224/1375
CVSSv3 Scoring		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
N/A	12-Dec-2024	7.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. CVE ID : CVE-2024-54508	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 45, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 44, https://	0-APP-MAC0- 241224/1376
Insertion of Sensitive Informatio n into Log File	12-Dec-2024	5.5	The issue was resolved by sanitizing logging. This issue is fixed in macOS Sequoia 15.2. An app may be able to access user- sensitive data. CVE ID : CVE-2024-54484	https:// support. apple.co m/en- us/1218 39	O-APP-MACO- 241224/1377
CVSSv3 Scoring		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
N/A	12-Dec-2024	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sequoia 15.2. An app may be able to access user-sensitive data. CVE ID : CVE-2024-54504	https:// support. apple.co m/en- us/1218 39	O-APP-MACO- 241224/1378
N/A	12-Dec-2024	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2. An app may be able to access sensitive user data. CVE ID : CVE-2024-54513	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 44, https://	O-APP-MACO- 241224/1379
N/A	12-Dec-2024	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.2. An	https:// support. apple.co m/en-	O-APP-MACO- 241224/1380

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			app may be able to bypass kASLR.	us/1218 39	
			CVE ID : CVE-2024-54531		
N/A	12-Dec-2024	3.3	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15.2. Privacy indicators for microphone access may be attributed incorrectly. CVE ID : CVE-2024-54493	https:// support. apple.co m/en- us/1218 39	O-APP-MACO- 241224/1381
Affected Vers	sion(s): * Up to	(including	y) 13.7.2		
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious app may be able to access private information. CVE ID : CVE-2024-54526	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43,	O-APP-MACO- 241224/1382
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
				https:// support. apple.co m/en- us/1218 44	
Affected Ver	sion(s): From (i	ncluding)	13.0 Up to (excluding) 13.7.2		
N/A	12-Dec-2024	7.8	A logic issue was addressed with improved file handling. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious app may be able to gain root privileges. CVE ID : CVE-2024-44291	https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	O-APP-MACO- 241224/1383
N/A	12-Dec-2024	6.5	This issue was addressed through improved state management. This issue is fixed in macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A user with screen sharing access may be able to view another user's screen. CVE ID : CVE-2024-44248	https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	O-APP-MACO- 241224/1384
N/A	12-Dec-2024	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, macOS Ventura 13.7.2, iOS 18.1 and	https:// support. apple.co m/en- us/1215	O-APP-MACO- 241224/1385

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 18.1, macOS Sonoma 14.7.2. Processing a malicious crafted file may lead to a denial-of-service. CVE ID : CVE-2024-44201	63, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	
N/A	12-Dec-2024	5.5	A logic issue was addressed with improved file handling. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access protected user data. CVE ID : CVE-2024-44300	https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	O-APP-MACO- 241224/1386
Affected Ver	<mark>sion(s): From (</mark> i	ncluding)	14.0 Up to (excluding) 14.7.2		I
N/A	12-Dec-2024	8.8	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2,	https:// support. apple.co m/en- us/1218	O-APP-MACO- 241224/1387
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
			macOS Sonoma 14.7.2. An app may be able to break out of its sandbox. CVE ID : CVE-2024-54498	39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	
N/A	12-Dec-2024	7.8	A logic issue was addressed with improved file handling. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious app may be able to gain root privileges. CVE ID : CVE-2024-44291	https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	O-APP-MACO- 241224/1388
N/A	12-Dec-2024	7.8	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Running a mount command may unexpectedly execute arbitrary code. CVE ID : CVE-2024-54489	https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40,	O-APP-MACO- 241224/1389

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https:// support. apple.co m/en- us/1218 42	
N/A	12-Dec-2024	7.1	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to overwrite arbitrary files. CVE ID : CVE-2024-54528	https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	O-APP-MACO- 241224/1390
N/A	12-Dec-2024	6.5	This issue was addressed through improved state management. This issue is fixed in macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A user with screen sharing access may be able to view another user's screen. CVE ID : CVE-2024-44248	https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	O-APP-MACO- 241224/1391
N/A	12-Dec-2024	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2,	https:// support. apple.co m/en- us/1218 37, https://	O-APP-MACO- 241224/1392

Concurrent Execution using Shared Resource with Improper synchroniz ationA race condition was addressed with additional vators 12.2 per 2024Macco Sonoma 14.7.2, apple.co m/en- us/1218 30, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 43Concurrent Execution using Shared Resource with Improper synchroniz ationA race condition was addressed with additional vations 15.2, i05 18.2 and iPadOS 18.2, macOS Sequeia 15.2, i05 18.2, macOS sequeia 15	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource withaddressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, support. apple.co 37,o-APP-MACO- 241224/1393 attacker may be able to oreate a read-only memory us/1218				macOS Sonoma 14.7.2. Processing a maliciously crafted font may result in the disclosure of process memory.	apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218	
Condition') mapping that can be written to. 38, https:// CVE ID : CVE-2024-54494 support. apple.co	Execution using Shared Resource with Improper Synchroniz ation ('Race	12-Dec-2024	5.9	addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory mapping that can be written to.	support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support.	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42,	
N/A	12-Dec-2024	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, macOS Ventura 13.7.2, iOS 18.1 and iPadOS 18.1, macOS Sonoma 14.7.2. Processing a malicious crafted file may lead to a denial-of-service. CVE ID : CVE-2024-44201	https:// support. apple.co m/en- us/1215 63, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en-	O-APP-MACO- 241224/1394

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Descri	ption & C	VE ID	Ра	tch	NCIII	PC ID
						us/1 42	1218		
N/A	12-Dec-2024	5.5	A logic issu with impro This issue Sequoia 15 Ventura 13 Sonoma 14 be able to a user data. CVE ID : C	oved file is fixed i 5.2, mac(5.7.2, ma 5.7.2, An access p	handling n macOS DS acOS app may rotected	sup app m/e us/ 39, http sup app m/e us/ 40, http sup app m/e	1218 port. le.co en- 1218 port. le.co	O-APP-I 241224	
N/A	12-Dec-2024	5.5	The issue v with impro issue is fix Sequoia 15 Ventura 13 Sonoma 14 be able to a sensitive d CVE ID : C	oved che ed in ma 5.2, mac 8.7.2, ma 4.7.2. An access u ata.	ecks. This acOS DS acOS app may ser-	sup app m/e us/ 39, http sup app m/e us/ 40, http sup app m/e	1218 port. le.co en- 1218 port. le.co	O-APP-1 241224	
N/A	12-Dec-2024	5.5	The issue with impro issue is fixe Sequoia 15 Ventura 13	oved che ed in ma 5.2, mac(cks. This cOS DS	sup app m/e	os:// port. le.co en- 1218	0-APP-1 241224	
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
N/A12-Dec-20245.5The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, wisionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS macOS Ventura 13.7.2, macOS Sonoma 14.7.2.o-APP-MACO 241224/13980-APP-MACO 241224/13980-APP-MACO 241224/13980-APP-MACO 241224/13980-APP-MACO macOS Ventura 13.7.2, macOS Sonoma 14.7.2.0-APP-MACO 241224/13980-APP-MACO 241224/13980-APP-MACO macOS Ventura 13.7.2, macOS Sonoma 14.7.2.0-APP-MACO 241224/1398				be able to access user- sensitive data.	https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218	
CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory. CVE ID : CVE-2024-54500	support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 40, https://	0-APP-MACO- 241224/1398

N/A12-Dec-20245.55.55.5Support support support support support support support support apple.co m/en- us/1218 37, https:// support apple.co m/en- us/1218 37, https:// support apple.co m/en- us/1218 39, https:// support apple.co m/en- us/1218 39, https:// support apple.co m/en- us/1218 39, https:// support apple.co m/en- us/1218 39, https:// support apple.co m/en- us/1218 39, https:// support apple.co m/en- us/1218 40, https:// support apple.co m/en- us/1218 43, https:// support apple.co m/en- us/1218 43, https:// support apple.co m/en- us/1218 43, https:// support apple.co m/en- us/1218 43, https:// support apple.co m/en- us/1218 43, https:// support apple.co m/en- us/1218 43, https:// support apple.co m/en- us/1218 43, https:// support apple.co m/en- us/1218 43, https:// support apple.co m/en- us/1218 43, https:// support apple.co m/en- us/1218 43, https:// support apple.co m/en- us/1218 43O-APP-MACO- 241224/1399Concurrent Execution 12-Dec-20245.1A race condition was addressed with improved support.O-APP-MACO- 241224/1400	N/A12-Dec-20245.55.5Fits issue was addressed with improved checks. This issue is fixed in watchOS Sequoia 15.2, iOS 18.2 and Delto 2013 12.2, maCOS Sonoma 14.7.2. An app may be able to access sensitive user data.https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 us/1218 com/en- us/1218 com/en- us/1218 com/en- us/1218 com/en- us/1218 com/en- us/1218 com/en- us/1218 com/en- us/1218 dotO-APP-MACO- ender apple.co m/en- us/1218 dotN/A12-Dec-20245.5Fits issue was addressed with improved checks. This issue is fixed in watchOS Sequoia 15.2, iOS 18.2, andOS Sonoma 14.7.2. An app may be able to access sensitive user data.O-APP-MACO- 241224/1399Concurrent12-Dec-20245.5A race condition washttps:// support. apple.co m/en- us/1218 dotConcurrent12-Dec-20245.1A race condition washttps://O-APP-MACO- 241224/1399	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A12-Dec-20245.517-ados 16.2, macos ventura 13.7.2, macos sonoma 14.7.2. An app may be able to access sensitive user data.https:// apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44241224/1399Concurrent12-Dec-20245.1A race condition washttps:// o0-APP-MACO- o o o o m/en- us/1218 d	N/A12-Dec-20245.517 adds 16.2, mators Ventura 13.7.2, mac0S Sonoma 14.7.2. An app may be able to access sensitive user data.https:// apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support.241224/1399Concurrent Execution12-Dec-20245.1A race condition was addressed with improvedhttps:// support.0-APP-MAC0- 241224/1400	Weakness	Publish Date	CVSSv3	This issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and	support. apple.co m/en- us/1218 43 https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218	
		Concurrent			Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access sensitive user data. CVE ID : CVE-2024-54527 A race condition was	us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44	241224/1399 0-APP-MACO-

using Shared Resource with Improper Synchroniz ation ('Race Condition') Iocking. This issue is fixed in iPadOS 17.7, watchOS Sequeia 15.2, iOS 18.2 and iPadOS 18.2, macOS Sonoma 14.7.2. An app may be able to leak sensitive kernel state. apple.co m/en- us/1218 CVE ID : CVE-2024-54510 38, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 Affected Version(s): From (including) 14.0 Up to (including) 14.7.2. N/A 12-Dec-2024 5.5 The issue was addressed with improve the cles. This issue is fixed in matchOS Sequeia 15.2, iOS 18.2, andOS Sonoma 14.7.2. An app may be able to leak sensitive kernel state. https:// support. apple.co m/en- us/1218 Affected Version(s): From (including) 14.0 Up to (including) 14.7.2 The issue was addressed with improved checks. This issue is fixed in matchOS Sequeia 15.2, iOS 18.2, and US_Sonoma 14.7.2. A malicious https:// support. apple.co m/en- us/1218 N/A 12-Dec-2024 5.5 The issue was addressed with improved checks. This issue is fixed in matchOS Sequeia 15.2, iOS 18.2, and S7, Ventura 13.7.2, macOS Sequeia 15.2, iOS 18.2, and S7, 0-APP-MACO- 241224/1401 VCXSV3 Scoreng Scale 01 12 12 12 12 14 14 14 15 15 15 15 15 15 15 15 15 15 15 15 15 15 <t< th=""><th>Weakness</th><th>Publish Date</th><th>CVSSv3</th><th>Description & CVE ID</th><th>Patch</th><th>NCIIPC ID</th></t<>	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
M/A Affected Version(s): From (including) 14.0 Up to (including) 14.7.2 https:// N/A I2-Dec-2024 The issue was addressed with improved checks. This issue is fixed in watchOS https:// apple.co 11.2, tvOS 18.2, macOS m/en- 0-APP-MACO- Sequoia 15.2, iOS 18.2 and us/1218 241224/1401 iPadOS 18.2, macOS 37, Ventura 13.7.2, macOS 37, Nttps:// Sonoma 14.7.2. A malicious support.	using Shared Resource with Improper Synchroniz ation ('Race	Publish Date	CVSSV3	locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to leak sensitive kernel state.	apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en-	
N/A 12-Dec-2024 5.5 with improved checks. This issue is fixed in watchOS supple.co apple.co 11.2, tvOS 18.2, macOS m/en- 0-APP-MACO- Sequoia 15.2, iOS 18.2 and us/1218 241224/1401 iPadOS 18.2, macOS 37, Ventura 13.7.2, macOS https:// Sonoma 14.7.2. A malicious support.	Affected Ver	<mark>sion(s): From (</mark> i	ncluding)	14.0 Up to (including) 14.7.2	43	
	N/A	12-Dec-2024	5.5	with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS	support. apple.co m/en- us/1218 37, https://	
STATUS TO LAU VERSIONS			1-2 2	-3 3-44-55-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			app may be able to access private information. CVE ID : CVE-2024-54526	apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https://	
Affected Ver	sion(s): From (i	ncluding)	15.0 Up to (excluding) 15.2		
N/A	12-Dec-2024	8.8	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to break out of its sandbox. CVE ID : CVE-2024-54498	https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support.	O-APP-MACO- 241224/1402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.co m/en- us/1218 42	
N/A	12-Dec-2024	7.8	A logic issue was addressed with improved file handling. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious app may be able to gain root privileges. CVE ID : CVE-2024-44291	https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	O-APP-MACO- 241224/1403
N/A	12-Dec-2024	7.8	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Running a mount command may unexpectedly execute arbitrary code. CVE ID : CVE-2024-54489	https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	O-APP-MACO- 241224/1404
N/A	12-Dec-2024	7.1	A logic issue was addressed with improved restrictions. This issue is fixed in macOS	https:// support. apple.co	O-APP-MACO- 241224/1405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to overwrite arbitrary files. CVE ID : CVE-2024-54528	m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	
N/A	12-Dec-2024	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted font may result in the disclosure of process memory. CVE ID : CVE-2024-54486	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en-	O-APP-MACO- 241224/1406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				42, https:// support. apple.co m/en- us/1218 43	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	12-Dec-2024	5.9	A race condition was addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory mapping that can be written to. CVE ID : CVE-2024-54494	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43	O-APP-MACO- 241224/1407
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2024	5.5	A logic issue was addressed with improved file handling. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access protected user data. CVE ID : CVE-2024-44300	https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	O-APP-MACO- 241224/1408
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access user- sensitive data. CVE ID : CVE-2024-54474	https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42	O-APP-MACO- 241224/1409
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may	https:// support. apple.co m/en- us/1218 39, https://	O-APP-MACO- 241224/1410

0-1

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

N/A 12-Dec-2024 5.5 The issue was addressed with improved checks. This issue is fixed in 1PadOS 11.2, vision05 2.2, tvOS 11.2, vision05 2.2, tvOS 11.2, vision05 2.2, tvOS 11.2, macOS Sequed 15.2, iOS 11.2, macOS ventura 13.7.2, macOS sequed 15.2, iOS 11.2, iS 11.2, macOS sequed 15.2, iOS 11.2, iS 11.	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A 12-Dec-2024 P.5 N/A 12-Dec-2024 P.5 N/A 12-Dec-2024 P.5 P.5 P.5 P.5 P.5 P.5 P.5 P.5				sensitive data.	apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218	
	N/A	12-Dec-2024	5.5	with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory.	support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m/en- us/1218 43	
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious app may be able to access private information. CVE ID : CVE-2024-54526	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43, https://	O-APP-MACO- 241224/1412
N/A	12-Dec-2024	5.5	This issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS	https:// support. apple.co m/en-	O-APP-MACO- 241224/1413

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

Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access sensitive user data.us/1218 37, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44Concurrent Execution using Shared Resource with Improper Synchroniz ation (Race Condition')A race condition was addressed with improved locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tv0S 18.2, andOS Sonom 14.7.2. An app may be able to leak sensitive with 23.2, iOS 18.2 and iPadOS 18.2, macOS Sonom 14.7.2. An app may be able to leak sensitive with 23.3, https:// support. apple.co m/en- us/1218 ipadOS 18.2, macOS Sonom 14.7.2. An app may be able to leak sensitive with 23.3, https:// support. apple.co m/en- us/1218 ipadOS 18.2, macOS Sonom 14.7.2. An app may be able to leak sensitive kernel state.0-APP-MACO- 241224/1414 apple.co m/en- us/1218 ipados ipadOS 18.2, macOS support. ipadOS 18.2, macOS support. ipadOS 1	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Execution using Shared Resource with12-Dec-20245.1A face condition was addressed with improved locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOSsupport. apple.co m/en- us/1218O-APP-MACO- 241224/1414Improper Synchroniz ation ('Race Condition')12-Dec-20245.1Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS0-APP-MACO- 241224/1414				iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access sensitive user data.	37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218	
	Execution using Shared Resource with Improper Synchroniz ation ('Race	12-Dec-2024	5.1	addressed with improved locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to leak sensitive	support. apple.co m/en- us/1218 37, https:// support. apple.co m/en-	

Origin Validation Error12-Dec-20245.3A cookie management issue management. This issue is fixed in Safari 18.1, visionOS 2.1, tvOS 18.1, iOS 18.1 and tros 18.1, visionOS 2.1, tvOS 18.1, iOS 18.1 and tros 18.1, visionOS 2.1, tvOS 18.1, iOS 18.1 and tros 18.1, visionOS 2.1, tvOS 18.1, iOS 18.1 and ple.co m/en- us/1218 d3https:// support. apple.co m/en- us/1218 d3Origin Validation Error12-Dec-20245.3A cookie management issue management. This issue is fixed in Safari 18.1, visionOS 2.1, tvOS 18.1, iOS 18.1 and ple.co m/en- us/1215 d3, https:// support. apple.co m/en- us/1215 d3, https:// support. apple.co m/en- us/1215 d3, https:// support. apple.co m/en- us/1215 d3, https:// support. apple.co m/en- us/1215 d3, https:// support. apple.co m/en- us/1215 d3, https:// support. apple.co m/en- us/1215 d3, https:// support. apple.co	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 18.1Affected Version(s): * Up to (excluding) 18.1A cookie management issuewas addressed withimproved statemanagement. This issue isfixed in Safari 18.1, visionOS2.1, tvOS 18.1, iOS 18.1 andiPadOS 18.1, watchOS 11.1.Cookies belonging to oneorigin may be sent toanother origin.CVE ID : CVE-2024-44212support.apple.coapple.co				CVE ID : CVE-2024-54510	support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218	
Origin Validation Error12-Dec-20245.35.3S.3Support. A cookie management issue was addressed with improved state fixed in Safari 18.1, visionOS 2.1, tvOS 18.1, iOS 18.1 and iPadOS 18.1, watchOS 11.1. Cookies belonging to one origin may be sent to another origin.support. apple.co m/en- us/1215 63, https:// support. apple.coO-APP-TVOS- 241224/1415			(excluding	g) 18.1		
m/en-us/1215 CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Origin Validation Error	12-Dec-2024	5.3	A cookie management issue was addressed with improved state management. This issue is fixed in Safari 18.1, visionOS 2.1, tvOS 18.1, iOS 18.1 and iPadOS 18.1, watchOS 11.1. Cookies belonging to one origin may be sent to another origin. CVE ID : CVE-2024-44212	support. apple.co m/en- us/1215 63, https:// support. apple.co m/en- us/1215 65, https:// support. apple.co m/en- us/1215	241224/1415

Out-of-bounds 9.8 The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2, and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. CVE ID : CVE-2024-54534 https:// support. apple.co m/en-us/1218 43, https:// support. apple.co m/en-us/1218 44, htttps// support. apple.co m/en-us/1218 44, https	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds12-Dec-20249.8The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, Processing maliciously crafted web content may lead to memory corruption.https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 additional common support. apple.co m/en- us/1218 additional common support. apple.co m/en- us/1218 additional common support. apple.co m/en- us/1218 additional common support. apple.co m/en- us/1218 additional common support. apple.co m/en- us/1218 additional common support.0-APP-TVOS- 241224/1416Out-of- us/1218 additional common support. apple.co m/en- us/1218 additional common support. apple.co m/en- us/1218					https:// support. apple.co m/en- us/1215 69, https:// support. apple.co m/en- us/1215	
Out-of- bounds12-Dec-20249.8Free issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption.0-APP-TVOS- 241224/1416 m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- 	Affected Ver	sion(s): * Up to	(excluding	g) 18.2		
	bounds	12-Dec-2024	9.8	with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption	support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				45, https:// support. apple.co m/en- us/1218 46	
Access of Resource Using Incompatib le Type ('Type Confusion')	12-Dec-2024	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. CVE ID : CVE-2024-54505	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co	O-APP-TVOS- 241224/1417
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 3-44-55-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2024	7.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. CVE ID : CVE-2024-54479	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co	O-APP-TVOS- 241224/1418
N/A	12-Dec-2024	7.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously	https:// support. apple.co m/en- us/1218 37, https:// support.	O-APP-TVOS- 241224/1419
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
			crafted web content may lead to an unexpected process crash. CVE ID : CVE-2024-54508	apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 45, https:// support. apple.co m/en- us/1218 45, https://	
N/A	12-Dec-2024	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Ventura 13.7.2, Processing a maliciously crafted font may result in the disclosure of process memory. CVE ID : CVE-2024-54486	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en-	O-APP-TVOS- 241224/1420
				m/en-	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	12-Dec-2024	5.9	A race condition was addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory mapping that can be written to. CVE ID : CVE-2024-54494	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co	0-APP-TVOS- 241224/1421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43	
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory. CVE ID : CVE-2024-54500	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co	O-APP-TVOS- 241224/1422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.co m/en- us/1218 43	
N/A	12-Dec-2024	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2. An app may be able to access sensitive user data. CVE ID : CVE-2024-54513	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 45	O-APP-TVOS- 241224/1423
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co	O-APP-TVOS- 241224/1424

0-1

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

pri	op may be able to access rivate information. VE ID : CVE-2024-54526	m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40,	
		https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, 44	
N/A 12-Dec-2024 5.5 iPa Ver Son be use	his issue was addressed ith improved checks. This sue is fixed in watchOS 1.2, tvOS 18.2, macOS equoia 15.2, iOS 18.2 and adOS 18.2, macOS entura 13.7.2, macOS onoma 14.7.2. An app may e able to access sensitive ser data. VE ID : CVE-2024-54527	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218	0-APP-TVOS- 241224/1425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	12-Dec-2024	5.1	A race condition was addressed with improved locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to leak sensitive kernel state. CVE ID : CVE-2024-54510	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218	0-APP-TVOS- 241224/1426

				support. apple.co m/en- us/1218 42,	
				https:// support. apple.co m/en- us/1218 43	
Product: visio	onos				
Affected Version	on(s): * Up to	(excluding	g) 2.1		
Origin Validation 1 Error 1	12-Dec-2024	5.3	A cookie management issue was addressed with improved state management. This issue is fixed in Safari 18.1, visionOS 2.1, tvOS 18.1, iOS 18.1 and iPadOS 18.1, watchOS 11.1. Cookies belonging to one origin may be sent to another origin. CVE ID : CVE-2024-44212	https:// support. apple.co m/en- us/1215 63, https:// support. apple.co m/en- us/1215 65, https:// support. apple.co m/en- us/1215 66, https:// support. apple.co m/en- us/1215 69, https:// support. apple.co m/en- us/1215 71	0-APP-VISI- 241224/1427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): * Up to (excluding) 2.2							
Out-of- bounds Write	12-Dec-2024	9.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. CVE ID : CVE-2024-54534	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 45, https:// support. apple.co m/en- us/1218 44,	O-APP-VISI- 241224/1428		
Access of Resource Using Incompatib le Type	12-Dec-2024	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2,	https:// support. apple.co m/en- us/1218 37,	O-APP-VISI- 241224/1429		

 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
('Type Confusion')			macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. CVE ID : CVE-2024-54505	https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 44, https://	
N/A	12-Dec-2024	7.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. CVE ID : CVE-2024-54479	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support.	O-APP-VISI- 241224/1430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co	
N/A CVSSv3 Scoring	12-Dec-2024 Scale 0-1	7.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. CVE ID : CVE-2024-54508	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en-	0-APP-VISI- 241224/1431

N/A 12-Dec-2024 6.5 The issue was addressed with improved checks. This issue is fixed in PadOS 11.2, visionOS 2.2, tvOS 11.2, macOS Sequeta 15.2, 10S 18.2 and IPadOS 11.2, visionOS 2.2, tvOS 11.2, macOS Sequeta 15.2, 10S 18.2 and IPadOS 18.2, macOS Ventura 13.7.2, macOS Sequeta 15.2, 10S 18.2 and IPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2, Processing a malicously crafted font may result in the disclosure of process memory. ••••••••••••••••••••••••••••••••••••	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A 12-Dec-2024 6.5 6.5 Fibe issue was addressed with improved checks. This issue is fixed in iPadOS 11.2, 38, visionOS 2.2, tvOS 18.2, https:// support. 18.2 and iPadOS 15.2, iOS 11.2, 38, visionOS 2.2, tvOS 18.2, https:// support. 18.2 and iPadOS 18.2, macOS Sequoia 15.2, iOS macOS Ventura 13.7.2, macOS Sonoma 14.7.2 us/1218 39, crafted font may result in the disclosure of process memory. CVE ID : CVE-2024-54486 140, https:// support. apple.co m/e-nus/1218 40, https:// support. apple.co m/e-nus/1218					44, https:// support. apple.co m/en- us/1218 45, https:// support. apple.co m/en- us/1218	
				with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted font may result in the disclosure of process memory. CVE ID : CVE-2024-54486	support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 40,	241224/1432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https:// support. apple.co m/en- us/1218 43 https://	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	12-Dec-2024	5.9	A race condition was addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory mapping that can be written to. CVE ID : CVE-2024-54494	support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43	O-APP-VISI- 241224/1433

4-5 3-4

5-6

8-9

9-10

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory. CVE ID : CVE-2024-54500	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43	O-APP-VISI- 241224/1434
N/A	12-Dec-2024	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2. An	https:// support. apple.co m/en- us/1218 37, https:// support.	O-APP-VISI- 241224/1435
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
				support. apple.co m/en- us/1215 69, https:// support. apple.co m/en- us/1215 71	
N/A	12-Dec-2024	3.3	This issue was addressed with improved redaction o sensitive information. This issue is fixed in iOS 18.1 an iPadOS 18.1, watchOS 11.1 An app may be able to determine a user's current location. CVE ID : CVE-2024-44290	d m/en- us/1215 63, https:// support. apple.co m/en-	O-APP-WATC- 241224/1437
Affected Vers	sion(s): * Up to	(excluding	g) 11.2		
Out-of- bounds Write	12-Dec-2024	9.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption CVE ID : CVE-2024-54534	support. apple.co m/en- us/1218 39, https:// support.	O-APP-WATC- 241224/1438
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
				support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 45, https:// support. apple.co m/en- us/1218 46	
Access of Resource Using Incompatib le Type ('Type Confusion')	12-Dec-2024	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. CVE ID : CVE-2024-54505	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co	0-APP-WATC- 241224/1439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m/en- us/1218 44, https:// support. apple.co m/en- us/1218 45	
N/A	12-Dec-2024	7.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. CVE ID : CVE-2024-54479	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en-	O-APP-WATC- 241224/1440

0-1

1-2

2-3

Page **526** of **1137**

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/1218 45	
N/A	12-Dec-2024	7.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. CVE ID : CVE-2024-54508	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 45, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 44, https:// support. apple.co m/en- us/1218 45, https:// support. apple.co	O-APP-WATC- 241224/1441
N/A	12-Dec-2024	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2,	https:// support. apple.co m/en- us/1218	O-APP-WATC- 241224/1442

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted font may result in the disclosure of process memory. CVE ID : CVE-2024-54486	37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42, https://	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	12-Dec-2024	5.9	A race condition was addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https://	O-APP-WATC- 241224/1443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mapping that can be written to. CVE ID : CVE-2024-54494	support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42,	
N/A CVSSv3 Scoring	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory. CVE ID : CVE-2024-54500	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co	0-APP-WATC- 241224/1444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43	
N/A	12-Dec-2024	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2. An app may be able to access sensitive user data. CVE ID : CVE-2024-54513	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en-	O-APP-WATC- 241224/1445

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
				us/1218 45	
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious app may be able to access private information. CVE ID : CVE-2024-54526	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43, https://	O-APP-WATC- 241224/1446
N/A	12-Dec-2024	5.5	This issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and	https:// support. apple.co m/en- us/1218	O-APP-WATC- 241224/1447

 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
			iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access sensitive user data. CVE ID : CVE-2024-54527	37, https:// support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43, https:// support. apple.co m/en- us/1218 43, https://	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	12-Dec-2024	5.1	A race condition was addressed with improved locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Ventura 13.7.2. An app may be able to leak sensitive kernel state. CVE ID : CVE-2024-54510	https:// support. apple.co m/en- us/1218 37, https:// support. apple.co m/en- us/1218 38, https://	O-APP-WATC- 241224/1448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				support. apple.co m/en- us/1218 39, https:// support. apple.co m/en- us/1218 40, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 42, https:// support. apple.co m/en- us/1218 43	
Vendor: Hu					
Product: ha					
Affected Ver Uncaught Exception	sion(s): 5.0.0 12-Dec-2024	7.1	Null pointer dereference vulnerability in the image decoding module Impact: Successful exploitation of this vulnerability will affect availability. CVE ID : CVE-2024-54106	https:// consum er.huaw ei.com/e n/suppo rt/bullet in/2024 /12/	O-HUA-HARM- 241224/1449
Improper Input Validation	12-Dec-2024	7.1	Read/Write vulnerability in the image decoding module Impact: Successful exploitation of this vulnerability will affect availability.	https:// consum er.huaw ei.com/e n/suppo rt/bullet	O-HUA-HARM- 241224/1450

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
			CVE ID : CVE-2024-54107	in/2024 /12/	
Improper Input Validation	12-Dec-2024	6.5	Read/Write vulnerability in the image decoding module Impact: Successful exploitation of this vulnerability will affect availability. CVE ID : CVE-2024-54108	https:// consum er.huaw ei.com/e n/suppo rt/bullet in/2024 /12/	O-HUA-HARM- 241224/1451
Improper Input Validation	12-Dec-2024	6.5	Read/Write vulnerability in the image decoding module Impact: Successful exploitation of this vulnerability will affect availability. CVE ID : CVE-2024-54109	https:// consum er.huaw ei.com/e n/suppo rt/bullet in/2024 /12/	O-HUA-HARM- 241224/1452
N/A	12-Dec-2024	6.5	Process residence vulnerability in abnormal scenarios in the print module Impact: Successful exploitation of this vulnerability may affect power consumption. CVE ID : CVE-2024-54113	https:// consum er.huaw ei.com/e n/suppo rt/bullet in/2024 /12/	O-HUA-HARM- 241224/1453
N/A	12-Dec-2024	6.2	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this vulnerability may affect service confidentiality. CVE ID : CVE-2024-54104	https:// consum er.huaw ei.com/e n/suppo rt/bullet in/2024 /12/	O-HUA-HARM- 241224/1454
Improper Privilege Manageme nt CVSSv3 Scoring	12-Dec-2024 Scale 0-1	6.2	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this	https:// consum er.huaw ei.com/e n/suppo rt/bullet	O-HUA-HARM- 241224/1455 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & C	VE ID	Patch	NCIIPC ID
			vulnerability may a service confidentia		in/2024 /12/	
			CVE ID : CVE-2024	-54110		
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	12-Dec-2024	6.2	Cross-process scree vulnerability in the UIExtension modul Impact: Successful exploitation of this vulnerability may a service confidentia CVE ID : CVE-2024	e Iffect lity.	https:// consum er.huaw ei.com/e n/suppo rt/bullet in/2024 /12/	241224/1456
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	12-Dec-2024	6.1	Vulnerability of imp access control in the module Impact: Successful exploitation of this vulnerability may a service confidentia CVE ID : CVE-2024	e album Iffect lity.	https:// consum er.huaw ei.com/e n/suppo rt/bullet in/2024 /12/	241224/1457
Insufficient Verificatio n of Data Authenticit y	12-Dec-2024	5.7	Read/Write vulner the image decoding Impact: Successful exploitation of this vulnerability will a availability. CVE ID : CVE-2024	g module ffect	https:// consum er.huaw ei.com/e n/suppo rt/bullet in/2024 /12/	241224/1458
N/A	12-Dec-2024	5.5	Cross-process scree vulnerability in the UIExtension modul Impact: Successful exploitation of this vulnerability may a service confidentia CVE ID : CVE-2024	e Iffect lity.	https:// consum er.huaw ei.com/e n/suppo rt/bullet in/2024 /12/	241224/1459
Buffer Copy without Checking Size of	12-Dec-2024	5.1	Read/Write vulnerability in the image decoding module Impact: Successful exploitation of this		https:// consum er.huaw ei.com/e n/suppo	
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Input ('Classic Buffer Overflow')			vulnerability will affect availability. CVE ID : CVE-2024-54105	rt/bullet in/2024 /12/		
Improper Check for Unusual or Exceptiona l Conditions	12-Dec-2024	4.4	Out-of-bounds access vulnerability in playback in the DASH module Impact: Successful exploitation of this vulnerability will affect availability. CVE ID : CVE-2024-54114	https:// consum er.huaw ei.com/e n/suppo rt/bullet in/2024 /12/	O-HUA-HARM- 241224/1461	
Improper Check for Unusual or Exceptiona l Conditions	12-Dec-2024	4.3	Out-of-bounds read vulnerability in the DASH module Impact: Successful exploitation of this vulnerability will affect availability. CVE ID : CVE-2024-54115	https:// consum er.huaw ei.com/e n/suppo rt/bullet in/2024 /12/	O-HUA-HARM- 241224/1462	
Improper Check for Unusual or Exceptiona l Conditions	12-Dec-2024	4.3	Out-of-bounds read vulnerability in the M3U8 module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. CVE ID : CVE-2024-54116	https:// consum er.huaw ei.com/e n/suppo rt/bullet in/2024 /12/	O-HUA-HARM- 241224/1463	
Vendor: Lin						
Product: lin						
Affected Version(s): * Up to (excluding) 6.11.10						
Double Free	04-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/6 825cb07 b79ffeb 1d90ffaa	O-LIN-LINU- 241224/1464	

3-4

4-5

5-6

6-7

7-8

8-9

9-10

0-1

1-2

	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drm/amd/display: Handle dml allocation failure to avoid crash	7a12274 62cdca3 4ae, https://	
			[Why] In the case where a dml allocation fails for any reason, the current state's dml contexts would no longer be valid. Then subsequent calls dc_state_copy_internal would shallow copy	git.kerne l.org/sta ble/c/8 74ff59cd e8fc525 112dda2 6b501a1 bac17dd e9f	
			invalid memory and if the new state was released, a double free would occur.		
			[How] Reset dml pointers in new_state to NULL and avoid invalid pointer		
			(cherry picked from commit bcafdc61529a48f6f06355d 78eb41b3aeda5296c) CVE ID : CVE-2024-53133		
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: x86/CPU/AMD: Clear virtualized VMLOAD/VMSAVE on Zen4 client	https:// git.kerne l.org/sta ble/c/0 0c713f8 4f477a8 5e524f3 4aad8fb d11a1c0 51f0,	O-LIN-LINU- 241224/1465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A number of Zen4 client SoCs advertise the ability to use virtualized VMLOAD/VMSAVE, but using these instructions is	https:// git.kerne l.org/sta ble/c/a5 ca1dc46 a6b610d	
			reported to be a cause of a random host reboot.	d4627d 8b633d 6c84f97	
			These instructions aren't intended to be advertised on Zen4 client	24ef0	
			so clear the capability.		
			CVE ID : CVE-2024-53114		
			In the Linux kernel, the following vulnerability has been resolved:		
			sched/task_stack: fix object_is_on_stack() for KASAN tagged pointers	https:// git.kerne l.org/sta ble/c/fb fe23012	
N/A	04-Dec-2024	5.5	When CONFIG_KASAN_SW_TAGS and CONFIG_KASAN_STACK are enabled, the	cec509d fbe0985 2019c4e 4bb849 99d0,	O-LIN-LINU-
	01 Dec 2021	5.5	object_is_on_stack() function may produce incorrect results due to the	https:// git.kerne l.org/sta	241224/1466
			presence of tags in the obj pointer, while the stack pointer does not have	ble/c/fd 7b4f9f4 6d46acb	
			tags. This discrepancy can lead to incorrect stack object detection and	c7af3a4 39bb0d 869efdc 5c58	
			subsequently trigger warnings if CONFIG_DEBUG_OBJECTS is also enabled.		

4-5 3-4

5-6

8-9

9-10

6-7

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Example of the warning:		
			ODEBUG: object 3eff800082ea7bb0 is NOT on stack ffff800082ea0000, but annotated.		
			[cut here]		
			WARNING: CPU: 0 PID: 1 at lib/debugobjects.c:557 debug_object_init+0x330/ 0x364		
			Modules linked in:		
			CPU: 0 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.12.0-rc5 #4		
			Hardware name: linux,dummy-virt (DT)		
			pstate: 600000c5 (nZCv daIF -PAN -UAO -TCO -DIT - SSBS BTYPE=)		
			pc : debug_object_init+0x330/ 0x364		
			lr : debug_object_init+0x330/ 0x364		
			sp : ffff800082ea7b40		
			x29: ffff800082ea7b40 x28: 98ff0000c0164518 x27: 98ff0000c0164534		
			x26: ffff800082d93ec8 x25: 0000000000000001 x24: 1cff0000c00172a0		
			x23: 0000000000000000 x22: ffff800082d93ed0 x21: ffff800081a24418		

3-4 4-5

5-6

6-7

8-9

9-10

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x20: 3eff800082ea7bb0 x19: efff800000000000 x18: 0000000000000000		
			x17: 000000000000000ff x16: 0000000000000047 x15: 206b63617473206e		
			x14: 0000000000000018 x13: ffff800082ea7780 x12: 0ffff800082ea78e		
			x11: 0ffff800082ea790 x10: 0ffff800082ea79d x9 : 34d77febe173e800		
			x8:34d77febe173e800 x7: 0000000000000001 x6: 0000000000000001		
			x5 : feff800082ea74b8 x4 : ffff800082870a90 x3 : ffff80008018d3c4		
			x2:0000000000000001 x1 :ffff800082858810 x0: 000000000000050		
			Call trace:		
			debug_object_init+0x330/ 0x364		
			debug_object_init_on_stack+ 0x30/0x3c		
			schedule_hrtimeout_range_c lock+0xac/0x26c		
			schedule_hrtimeout+0x1c/ 0x30		
			wait_task_inactive+0x1d4/0 x25c		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kthread_bind_mask+0x28/0 x98 init_rescuer+0x1e8/0x280		
			workqueue_init+0x1a0/0x3		
			kernel_init_freeable+0x118 /0x200 kernel_init+0x28/0x1f0 ret_from_fork+0x10/0x20		
			[end trace 0000000000000000]		
			ODEBUG: object 3eff800082ea7bb0 is NOT on stack ffff800082ea0000, but annotated.		
			[cut here] CVE ID : CVE-2024-53128		
Affected Vers	sion(s): * Up to	(excluding			
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/0a	
Out-of-	02-Dec-2024		drm/amd/display: Adjust VSDB parser for replay feature	326fbc8f 72a3200 51f2732 8d4d4e7	
bounds 02-Dec-2024 Read		7.1	At some point, the IEEE ID identification for the replay check in the	abdfe68 d7, https:// git.kerne l.org/sta	O-LIN-LINU- 241224/1467
		AMD EDID was added. However, this check causes the following out-of-bounds issues when using KASAN:	ble/c/1 6dd282 5c23530 f2259fc6		
CVSSv3 Scoring	Scale 0-1	1-2 2	using KASAN:	71960a3	8-9 9-10
*stands for all v					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			 [27.804016] BUG: KASAN: slab-out-of-bounds in amdgpu_dm_update_freesy nc_caps+0xefa/0x17a0 [amdgpu] [27.804788] Read of size 1 at addr ffff8881647fdb00 by task systemd-udevd/383 	a65d2af 69bd, https:// git.kerne l.org/sta ble/c/8 db8670 61f4c76 505ad62 422b65 d666b4 528921 7	
			[27.821207] Memory state around the buggy address:		
			[27.821215] ffff8881647fda00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
			[27.821224] ffff8881647fda80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
			[27.821234] >ffff8881647fdb00: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc		
			[27.821243] ^		
			[27.821250] ffff8881647fdb80: fc fc fc fc fc fc		
			[27.821259] ffff8881647fdc00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
			[27.821268]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This is caused because the ID extraction happens outside of the range of the edid lenght. This commit addresses this issue by considering the amd_vsdb_block size.		
			(cherry picked from commit b7e381b1ccd5e778e3d9c4 4c669ad38439a861d8)		
Affected Ver	sion(s): * Up to	(including	CVE ID : CVE-2024-53108		
			In the Linux kernel, the	https://	
			following vulnerability has been resolved: vdpa: solidrun: Fix UB bug with devres	git.kerne l.org/sta ble/c/0 b364cf5 3b2020 4e92bac	
			In psnet_open_pf_bar() and snet_open_vf_bar() a string later passed to pcim_iomap_regions() is	7c6ebd1 ee7d3ec 62931, https:// git.kerne	O-LIN-LINU-
N/A	04-Dec-2024	7.8	placed on the stack. Neither pcim_iomap_regions() nor the functions it calls copy that string.	l.org/sta ble/c/5 bb287da 2d2d5b b8f7376 e223b02	241224/1468
			Should the string later ever be used, this, consequently, causes undefined behavior since the stack frame will by then have disappeared.	edb1699 8982e, https:// git.kerne l.org/sta ble/c/d 372dd0	
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
			Fix the bug by allocating the strings on the heap through devm_kasprintf(). CVE ID : CVE-2024-53126	9cfbf132 4f54cbff d81fcaf6 cdf3e60 8e	
Affected Ver	sion(s): 6.12		1		
Double Free	04-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Handle dml allocation failure to avoid crash [Why] In the case where a dml allocation fails for any reason, the current state's dml contexts would no longer be valid. Then subsequent calls dc_state_copy_internal would shallow copy invalid memory and if the new state was released, a double free would occur. [How] Reset dml pointers in new_state to NULL and avoid invalid pointer	https:// git.kerne l.org/sta ble/c/6 825cb07 b79ffeb 1d90ffaa 7a12274 62cdca3 4ae, https:// git.kerne l.org/sta ble/c/8 74ff59cd e8fc525 112dda2 6b501a1 bac17dd e9f	O-LIN-LINU- 241224/1469

5-6 6-7 8-9

7-8

9-10

3-4

1-2

2-3

Use After Free04-Dec-20247.87.8(cherry picked from commit bcafdc61529a48/6/063554 78cb41b3ad62296c) CVE ID : CVE-2024-53133https:// git.kerne log/2014 ble/c/0 5656a66 592759 1010000000000000000000000000000000000	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free04-Dec-20247.8In the Linux kernel, the following vulnerability has been resolved:https:// git.kerne l.org/sta ble/c/0Use After Free04-Dec-20247.87.810Use After Free04-Dec-20247.81104-Dec-20247.8100-LIN-LINU- 241224/147004-Dec-20247.81004-Dec-20241004-Dec-2024 <td></td> <td></td> <td></td> <td>bcafdc61529a48f6f06355d</td> <td></td> <td></td>				bcafdc61529a48f6f06355d		
Use After Free04-Dec-20247.8following vulnerability has been resolved:https:// git.kerne lorg/sta ble/c/0 502759 242C740 242C740 636162 91b727 91b727 411b26 htat sctp_v6_available() is of alling dev_get_by_index_rcu()https:// git.kerne lorg/sta ble/c/0 502759 242C740 036162 91b727 91b727 91b727 91b727 91b727 91b727 91b727 1411b26 hts sctp_v6_available() is git.kerne https:// https:// git.kerne https:// git.kerne https:// git.kerne https:// git.kerne https:// git.kerne https:// git.kerne https:// git.kerne https:// git.kerne https:// https:// https:// https:// https:// https:// https:// https:// https:// https:// https:// https:// https:// https:// https:// https:// <br< td=""><td></td><td></td><td></td><td>CVE ID : CVE-2024-53133</td><td></td><td></td></br<>				CVE ID : CVE-2024-53133		
other info that might help		04-Dec-2024	7.8	CVE ID : CVE-2024-53133 In the Linux kernel, the following vulnerability has been resolved: sctp: fix possible UAF in sctp_v6_available() A lockdep report [1] with CONFIG_PROVE_RCU_LIST= y hints that sctp_v6_available() is calling dev_get_by_index_rcu() and ipv6_chk_addr() without holding rcu. [1] ======== WARNING: suspicious RCU usage 6.12.0-rc5-virtme #1216 Tainted: G W 	git.kerne l.org/sta ble/c/0 56556a66 592759 242c740 636162 91b727 4d11b2f, https:// git.kerne l.org/sta ble/c/ad 975697 211f4f2c 4ce61c3 ba524fd 14d88ce ab8, https:// git.kerne l.org/sta ble/c/eb 72e7fcc 83987d 5d5595 b43222f 23b295	
us debug this:						

0-1

1-2

2-3

4-5 5-6 6-7

9-10

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rcu_scheduler_active = 2, debug_locks = 1		
			1 lock held by sctp_hello/31495:		
			#0: ffff9f1ebbdb7418 (sk_lock-AF_INET6){+.+.}- {0:0}, at: sctp_bind (./arch/x86/include/asm/j ump_label.h:27 net/sctp/socket.c:315) sctp		
			stack backtrace:		
			CPU: 7 UID: 0 PID: 31495 Comm: sctp_hello Tainted: G W 6.12.0-rc5- virtme #1216		
			Tainted: [W]=WARN		
			Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian- 1.16.3-2 04/01/2014		
			Call Trace:		
			<task></task>		
			dump_stack_lvl (lib/dump_stack.c:123)		
			lockdep_rcu_suspicious (kernel/locking/lockdep.c:6 822)		
			dev_get_by_index_rcu (net/core/dev.c:876 (discriminator 7))		
			sctp_v6_available (net/sctp/ipv6.c:701) sctp		
			sctp_do_bind (net/sctp/socket.c:400 (discriminator 1)) sctp		
			sctp_bind (net/sctp/socket.c:320) sctp		
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
			inet6_bind_sk (net/ipv6/af_inet6.c:465)		
			? security_socket_bind (security/security.c:4581 (discriminator 1))		
			sys_bind (net/socket.c:1848 net/socket.c:1869)		
			? do_user_addr_fault (./include/linux/rcupdate.h :347		
			./include/linux/rcupdate.h:880./include/linux/mm.h:729arch/x86/mm/fault.c:1340)		
			? do_user_addr_fault (./arch/x86/include/asm/p reempt.h:84 (discriminator 13)		
			./include/linux/rcupdate.h: 98 (discriminator 13) ./include/linux/rcupdate.h: 882 (discriminator 13) ./include/linux/mm.h:729 (discriminator 13) arch/x86/mm/fault.c:1340 (discriminator 13))		
			x64_sys_bind (net/socket.c:1877 (discriminator 1) net/socket.c:1875 (discriminator 1) net/socket.c:1875 (discriminator 1))		
			do_syscall_64 (arch/x86/entry/common.c :52 (discriminator 1) arch/x86/entry/common.c: 83 (discriminator 1))		
			entry_SYSCALL_64_after_hw frame		
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
			(arch/x86/entry/entry_64. S:130)		
			RIP: 0033:0x7f59b934a1e7		
			Code: 44 00 00 48 8b 15 39		
			8c 0c 00 f7 d8 64 89 02 b8 ff		
			ff ff ff eb bd 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 b8		
			31 00 00 00 0f 05 <48> 3d		
			01 f0 ff ff 73 01 c3 48 8b 0d 09 8c 0c 00 f7 d8 64 89 01		
			48		
			All code		
			======		
			0: 44 00 00 add %r8b,(%rax)		
			3: 48 8b 15 39 8c 0c 00		
			mov		
			0xc8c39(%rip),%rdx # 0xc8c43		
			a: f7 d8 neg		
			%eax		
			c: 64 89 02 mov		
			%eax,%fs:(%rdx)		
			f: b8 ff ff ff ff mov \$0xffffffff,%eax		
			14: eb bd jmp 0xfffffffffffffd3		
			16: 66 2e 0f 1f 84 00 00		
			cs nopw 0x0(%rax,%rax,1)		
			1d: 00 00 00		
			20: 0f 1f 00		
			nopl (%rax)		
			23: b8 31 00 00 00 mov \$0x31,%eax		
			28: 0f 05 syscall		
			2a:* 48 3d 01 f0 ff ff		
			cmp		
CVSSv3 Scoring		1-2 2	<mark>-3</mark> 3-4 4-5 5-6 6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			\$0xfffffffffffff001,%rax < trapping instruction		
			30: 73 01 jae 0x33		
			32: c3 ret		
			33: 48 8b 0d 09 8c 0c 00 mov		
			0xc8c09(%rip),%rcx # 0xc8c43		
			3a: f7 d8 neg %eax		
			3c: 64 89 01 mov		
			%eax,%fs:(%rcx) 3f: 48 rex.W		
			3f: 48 rex.W		
			Code starting with the faulting instruction		
			=======================================		
			0: 48 3d 01 f0 ff ff		
			cmp \$0xffffffffffff001,%rax		
			6: 73 01 jae 0x9		
			8: c3 ret		
			9: 48 8b 0d 09 8c 0c 00		
			mov 0xc8c09(%rip),%rcx # 0xc8c19		
			10: f7 d8 neg %eax		
			12: 64 89 01		
			mov %eax,%fs:(%rcx)		
			15: 48 rex.W		

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RSP: 002b:00007ffe2d0ad398 EFLAGS: 00000202 ORIG_RAX: 000000000000031		
			RAX: ffffffffffffffda RBX: 00007ffe2d0ad3d0 RCX: 00007f59b934a1e7		
			RDX: 0000000000000001c RSI: 00007ffe2d0ad3d0 RDI: 00000000000000005		
			RBP: 0000000000000005 R08: 19999999999999999 R09: 000000000000000000		
			R10: 00007f59b9253298 R11: 000000000000		
			truncated		
			CVE ID : CVE-2024-53139		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/0a	
			drm/amd/display: Adjust VSDB parser for replay feature	326fbc8f 72a3200 51f2732 8d4d4e7 abdfe68	
Out-of- bounds Read	02-Dec-2024	7.1	At some point, the IEEE ID identification for the replay check in the	d7, https:// git.kerne l.org/sta	O-LIN-LINU- 241224/1471
			AMD EDID was added. However, this check causes the following	ble/c/1 6dd282 5c23530 f2259fc6	
			out-of-bounds issues when using KASAN:	71960a3 a65d2af 69bd,	
			[27.804016] BUG: KASAN: slab-out-of-bounds in amdgpu_dm_update_freesy	https:// git.kerne l.org/sta ble/c/8	
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
			nc_caps+0xefa/0x17a0 [amdgpu] [27.804788] Read of size 1 at addr ffff8881647fdb00 by task systemd-udevd/383	db8670 61f4c76 505ad62 422b65 d666b4 528921 7	
			[27.821207] Memory state around the buggy address:		
			[27.821215] ffff8881647fda00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
			[27.821224] ffff8881647fda80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
			[27.821234] >ffff8881647fdb00: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc		
			[27.821243] ^ [27.821250] ffff8881647fdb80: fc fc fc fc fc fc fc fc fc fc fc fc fc fc		
			[27.821259] ffff8881647fdc00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
			[27.821268] ====================================		
			===		

CVSSv3 Scoring Scale 0-1

5-6 6-7 8-9

9-10

7-8

*stands for all versions

3-4

2-3

1-2

PC ID
O-LIN-LINU-
/1472

tracing is disabled, and *stays* disabled prior to	
VM-Enter, which is	
necessary as hardware disallows loading (the guest's) RTIT_CTL if tracing	
is enabled (enforced via a VMX consistency check). Per the SDM:	
If the logical processor is operating with Intel PT enabled (if	
IA32_RTIT_CTL.TraceEn = 1) at the time of VM entry, the "load	
IA32_RTIT_CTL" VM-entry control must be 0.	
On the host side, KVM doesn't validate the guest CPUID configuration	
provided by userspace, and even worse, uses the guest configuration to	
decide what MSRs to save/load at VM-Enter and VM-Exit. E.g. configuring	
guest CPUID to enumerate more address ranges than are supported in hardware	
will result in KVM trying to passthrough, save, and load non-existent MSRs,	
which generates a variety of WARNs, ToPA ERRORs in the host, a potential	
deadlock, etc.	
CVE ID : CVE-2024-53135 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
Integer Overflow or Wraparoun d	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fs/proc/task_mmu: prevent integer overflow in pagemap_scan_get_args() The "arg->vec_len" variable is a u64 that comes from the user at the start of the function. The "arg- >vec_len * sizeof(struct page_region))" multiplication can lead to integer wrapping. Use size_mul() to avoid that. Also the size_add/mul() functions work on unsigned long so for 32bit systems we need to ensure that "arg->vec_len" fits in an unsigned long. CVE ID : CVE-2024-53107	https:// git.kerne l.org/sta ble/c/6 69b0cb8 1e4e4e7 8cff77a5 b367c7f 70c0c6c 05e, https:// git.kerne l.org/sta ble/c/ad ee03f89 03c58a6 a559f21 388a430 211fac8 ce9	O-LIN-LINU- 241224/1473
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nommu: pass NULL argument to vma_iter_prealloc() When deleting a vma entry from a maple tree, it has to pass NULL to	https:// git.kerne l.org/sta ble/c/2 47d720 b2c5d22 f728143 7fd6054 a138256 986ba, https:// git.kerne l.org/sta ble/c/8	O-LIN-LINU- 241224/1474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<pre>vma_iter_prealloc() in order to calculate internal state of the tree, but it passed a wrong argument. As a result, nommu kernels crashed upon accessing a vma iterator, such as acct_collect() reading the size of vma entries after do_munmap(). This commit fixes this issue by passing a right argument to the preallocation call.</pre>	bbf0ab6 31cdf1d ade6745 f137cff9 8751e6c ed7, https:// git.kerne l.org/sta ble/c/ac eaf33b7 666b72 dfb86e0 aa977be 81e3bcb c727	
N/A	02-Dec-2024	5.5	CVE ID : CVE-2024-53109 In the Linux kernel, the following vulnerability has been resolved: vp_vdpa: fix id_table array not null terminated error Allocate one extra virtio_device_id as null terminator, otherwise vdpa_mgmtdev_get_classes() may iterate multiple times and visit undefined memory. CVE ID : CVE-2024-53110	https:// git.kerne l.org/sta ble/c/0a 886489 d27459 6ad1a80 789d3a7 735032 10a615, https:// git.kerne l.org/sta ble/c/4e 39ecadf 1d2a081 871396 19f1f31 4b64ba7 d947, https:// git.kerne l.org/sta ble/c/8 70d68fe	O-LIN-LINU- 241224/1475

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				17b5d9 032049 dcad98b 5781a34 4a8657	
Integer Overflow or Wraparoun d	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/mremap: fix address wraparound in move_page_tables() On 32-bit platforms, it is possible for the expression `len + old_addr < old_end` to be false-positive if `len + old_addr` wraps around. `old_addr` is the cursor in the old range up to which page table entries have been moved; so if the operation succeeded, `old_addr` is the *end* of the old region, and adding `len` to it can wrap. The overflow causes mremap() to mistakenly believe that PTEs have been copied; the consequence is that mremap() bails out, but doesn't move the PTEs back before the new VMA is unmapped, causing anonymous pages in the	https:// git.kerne l.org/sta ble/c/9 09543dc 279a911 22fb08e 4653a72 b82f0ad 28f4, https:// git.kerne l.org/sta ble/c/a4 a282daf 1a190f0 3790bf1 63458ea 3c8d28d 217	O-LIN-LINU- 241224/1476

5-6 6-7 7-8

8-9

9-10

versions

0-1

1-2

4-5

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			region to be lost. So basically if userspace tries to mremap() a		
			private-anon region and hits this bug, mremap() will return an error and		
			the private-anon region's contents appear to have been zeroed.		
			The idea of this check is that `old_end - len` is the original start		
			address, and writing the check that way also makes it easier to read; so		
			fix the check by rearranging the comparison accordingly.		
			(An alternate fix would be to refactor this function by introducing an		
			"orig_old_start" variable or such.)		
			Tested in a VM with a 32-bit X86 kernel; without the patch:		
			user@horn:~/big_mremap\$ cat test.c		
			#define _GNU_SOURCE		
			<pre>#include <stdlib.h></stdlib.h></pre>		
			<pre>#include <stdio.h></stdio.h></pre>		
			#include <err.h></err.h>		

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<pre>#include <sys mman.h=""></sys></pre>		
			#define ADDR1		
			((void*)0x6000000)		
			#define ADDR2 ((void*)0x10000000)		
			#define SIZE		
			0x50000000uL		
			int main(void) {		
			unsigned char *p1 =		
			mmap(ADDR1, SIZE, PROT_READ PROT_WRITE,		
			MAP_ANONYMOUS MAP_PR		
			IVATE MAP_FIXED_NOREPL		
			ACE, -1, 0);		
			if (p1 == MAP_FAILED)		
			err(1, "mmap 1");		
			unsigned char *p2 = mmap(ADDR2, SIZE,		
			PROT_NONE,		
			MAP_ANONYMOUS MAP_PR IVATE MAP_FIXED_NOREPL		
			ACE, -1, 0);		
			if (p2 == MAP_FAILED)		
			err(1, "mmap 2");		
			*p1 = 0x41;		
			printf("first char is		
			0x%02hhx\n", *p1);		
			unsigned char *p3 = mremap(p1, SIZE, SIZE,		
			MREMAP_MAYMOVE MRE		
			MAP_FIXED, p2);		
			if (p3 == MAP_FAILED) {		

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
			<pre>printf("mremap() failed; first char is 0x%02hhx\n", *p1);</pre>		
			} else {		
			printf("mremap() succeeded; first char is 0x%02hhx\n", *p3);		
			}		
			}		
			user@horn:~/big_mremap\$ gcc -static -o test test.c		
			user@horn:~/big_mremap\$ setarch -R ./test		
			first char is 0x41		
			mremap() failed; first char is 0x00		

			With the patch:		
			user@horn:~/big_mremap\$ setarch -R ./test		
			first char is 0x41		
			mremap() succeeded; first char is 0x41		
			CVE ID : CVE-2024-53111	https://	
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/6	
N/A	02-Dec-2024	5.5	ocfs2: uncache inode which has failed entering the group	20d225 98110b 0d0cb97 a3fcca65	O-LIN-LINU- 241224/1477
				fc473ea 86e73,	
CVSSv3 Scoring *stands for all v		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
			Syzbot has reported the following BUG:	https:// git.kerne l.org/sta	
			kernel BUG at fs/ocfs2/uptodate.c:509!	ble/c/7 37f3413 7844d6	
			 Call Trace: <task></task>	572ab7d 473c998 c7f977ff 30eb,	
			?die_body+0x5f/0xb0	https:// git.kerne	
			? die+0x9e/0xc0	l.org/sta	
			? do_trap+0x15a/0x3a0 2	ble/c/8 43dfc80	
			ocfs2_set_new_buffer_uptod ate+0x145/0x160	4af4b33 8ead423	
			? do_error_trap+0x1dc/0x2c 0	31dd58 081b42 8ecdf8	
			? ocfs2_set_new_buffer_uptod ate+0x145/0x160		
			? pfx_do_error_trap+0x10/0 x10		
			? handle_invalid_op+0x34/0x 40		
			? ocfs2_set_new_buffer_uptod ate+0x145/0x160		
			? exc_invalid_op+0x38/0x50		
			? asm_exc_invalid_op+0x1a/0 x20		
			? ocfs2_set_new_buffer_uptod ate+0x2e/0x160		

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
			? ocfs2_set_new_buffer_uptod ate+0x144/0x160 ? ocfs2_set_new_buffer_uptod		
			ate+0x145/0x160		
			ocfs2_group_add+0x39f/0x 15a0		
			? pfx_ocfs2_group_add+0x1 0/0x10		
			? pfx_lock_acquire+0x10/0x 10		
			? mnt_get_write_access+0x68 /0x2b0		
			? pfx_lock_release+0x10/0x 10		
			? rcu_read_lock_any_held+0x b7/0x160		
			? pfx_rcu_read_lock_any_hel d+0x10/0x10		
			? smack_log+0x123/0x540 ?		
			mnt_get_write_access+0x68 /0x2b0 2		
			? mnt_get_write_access+0x68 /0x2b0		
			? mnt_get_write_access+0x22 6/0x2b0		
			ocfs2_ioctl+0x65e/0x7d0		

0-1

1-2

2-3

4-5 3-4 5-6

8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? pfx_ocfs2_ioctl+0x10/0x1 0		
			? smack_file_ioctl+0x29e/0x3 a0		
			? pfx_smack_file_ioctl+0x10 /0x10		
			? lockdep_hardirqs_on_prepa re+0x43d/0x780		
			? pfx_lockdep_hardirqs_on_ prepare+0x10/0x10		
			? pfx_ocfs2_ioctl+0x10/0x1 0		
			se_sys_ioctl+0xfb/0x170 do_syscall_64+0xf3/0x230		
			entry_SYSCALL_64_after_hw frame+0x77/0x7f		
			When 'ioctl(OCFS2_IOC_GROUP_A DD,)' has failed for the particular		
			inode in 'ocfs2_verify_group_and_inp ut()', corresponding buffer head		
			remains cached and subsequent call to the same 'ioctl()' for the same		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inode issues the BUG() in 'ocfs2_set_new_buffer_upto date()' (trying		
			to cache the same buffer head of that inode). Fix this by uncaching		
			the buffer head with 'ocfs2_remove_from_cache()' on error path in		
			'ocfs2_group_add()'.		
			CVE ID : CVE-2024-53112		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta	
			mm: fix NULL pointer dereference in alloc_pages_bulk_noprof	ble/c/3 150237 4627ba9 ec3e710 dbd0bb	
			We triggered a NULL pointer dereference for ac.preferred_zoneref->zone in	00457cc 6d2c19, https:// git.kerne l.org/sta	
NULL Pointer Dereferenc e	02-Dec-2024	02-Dec-2024 5.5	alloc_pages_bulk_noprof() when the task is migrated between cpusets.	ble/c/6a ddb2d9 501ec86 6d7b3a3 b4e6653 07c437e 9be2, https://	O-LIN-LINU- 241224/1478
			When cpuset is enabled, in prepare_alloc_pages(), ac- >nodemask may be		
		¤t->mems_allowed. when first_zones_zonelist() is called to find	git.kerne l.org/sta ble/c/8c		
			preferred_zoneref, the ac- >nodemask may be modified concurrently if the	e41b0f9 d77cca0 74df25a fd39b86	
			task is migrated between different cpusets. Assuming we have 2 NUMA Node,	e2ee3aa 68e	
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
			when traversing Node1 in ac->zonelist, the nodemask is 2, and when		
			traversing Node2 in ac- >zonelist, the nodemask is 1. As a result, the		
			ac->preferred_zoneref points to NULL zone.		
			In alloc_pages_bulk_noprof(), for_each_zone_zonelist_nod emask() finds a		
			allowable zone and calls zonelist_node_idx(ac.prefer red_zoneref), leading		
			to NULL pointer dereference.		
			alloc_pages_noprof() fixes this issue by checking NULL pointer in commit		
			ea57485af8f4 ("mm, page_alloc: fix check for NULL preferred_zone") and		
			commit df76cee6bbeb ("mm, page_alloc: remove redundant checks from alloc		
			fastpath").		
			To fix it, check NULL pointer for preferred_zoneref->zone.		
			CVE ID : CVE-2024-53113		
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/0	O-LIN-LINU- 241224/1479
CVSSv3 Scoring		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
			x86/CPU/AMD: Clear virtualized VMLOAD/VMSAVE on Zen4 client	0c713f8 4f477a8 5e524f3 4aad8fb d11a1c0 51f0,	
			A number of Zen4 client SoCs advertise the ability to use virtualized VMLOAD/VMSAVE, but using these instructions is reported to be a cause	https:// git.kerne l.org/sta ble/c/a5 ca1dc46 a6b610d d4627d	
			of a random host reboot.	8b633d 6c84f97 24ef0	
			These instructions aren't intended to be advertised on Zen4 client		
			so clear the capability.		
			CVE ID : CVE-2024-53114		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/3	
NULL			drm/vmwgfx: avoid null_ptr_deref in vmw_framebuffer_surface_c reate_handle	6f64da0 805551 75b58d 85f99f5f 90435e2	
Pointer Dereferenc e	02-Dec-2024 5.5	The 'vmw_user_object_buffer' function may return NULL with incorrect	74e56, https:// git.kerne l.org/sta ble/c/9	O-LIN-LINU- 241224/1480	
			inputs. To avoid possible null pointer dereference, add a check whether	3d1f41a 82de382 845af46	
			the 'bo' is NULL in the vmw_framebuffer_surface_c reate_handle.	0bf03bc b17dcbf 08c5	

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
			CVE ID : CVE-2024-53115		
			In the Linux kernel, the following vulnerability has been resolved: drm/panthor: Fix handling of partial GPU mapping of BOs		
N/A	02-Dec-2024	5.5	 bus This commit fixes the bug in the handling of partial mapping of the buffer objects to the GPU, which caused kernel warnings. Panthor didn't correctly handle the case where the partial mapping spanned multiple scatterlists and the mapping offset didn't point to the 1st page of starting scatterlist. The offset variable was not cleared after reaching the starting scatterlist. Following warning messages were seen. WARNING: CPU: 1 PID: 650 at drivers/iommu/iopgtable-arm.c:659arm_lpae_unmap+0x254/ 0x5a0 	https:// git.kerne l.org/sta ble/c/3 387e043 918e154 ca08d83 954966a 8b087fe 2835, https:// git.kerne l.org/sta ble/c/d 3e61af6 4b770e0 038470c 81f42bd 1d0598f 6bcc	O-LIN-LINU- 241224/1481

0-1

1-2

2-3

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pc : arm_lpae_unmap+0x254/ 0x5a0		
			lr : arm_lpae_unmap+0x2cc/0 x5a0		
			<snip></snip>		
			Call trace:		
			arm_lpae_unmap+0x254/ 0x5a0		
			arm_lpae_unmap+0x108/ 0x5a0		
			arm_lpae_unmap+0x108/ 0x5a0		
			arm_lpae_unmap+0x108/ 0x5a0		
			arm_lpae_unmap_pages+0x 80/0xa0		
			panthor_vm_unmap_pages+ 0xac/0x1c8 [panthor]		
			panthor_gpuva_sm_step_un map+0x4c/0xc8 [panthor]		
			op_unmap_cb.isra.23.constp rop.30+0x54/0x80		
			drm_gpuvm_sm_unmap+0 x184/0x1c8		
			drm_gpuvm_sm_unmap+0x 40/0x60		

3-4

4-5

5-6

6-7

9-10

2-3

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			panthor_vm_exec_op+0xa8/ 0x120 [panthor]		
			panthor_vm_bind_exec_sync _op+0xc4/0xe8 [panthor]		
			panthor_ioctl_vm_bind+0x1 0c/0x170 [panthor]		
			drm_ioctl_kernel+0xbc/0x1 38		
			drm_ioctl+0x210/0x4b0		
			_arm64_sys_ioctl+0xb0/0xf 8		
			invoke_syscall+0x4c/0x110		
			el0_svc_common.constprop. 1+0x98/0xf8		
			do_el0_svc+0x24/0x38		
			el0_svc+0x34/0xc8		
			el0t_64_sync_handler+0xa0 /0xc8		
			el0t_64_sync+0x174/0x178		
			<snip></snip>		
			panthor : [drm] drm_WARN_ON(unmapped_ sz != pgsize * pgcount)		
			WARNING: CPU: 1 PID: 650 at drivers/gpu/drm/panthor/		
			panthor_mmu.c:922 panthor_vm_unmap_pages+ 0x124/0x1c8 [panthor]		
			<snip></snip>		

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		pc: panthor_vm_unmap_pages+ 0x124/0x1c8 [panthor] lr: panthor_vm_unmap_pages+ 0x124/0x1c8 [panthor]		
		<snip> panthor : [drm] *ERROR* failed to unmap range ffffa388f000-ffffa3890000 (requested range ffffa388c000-ffffa3890000)</snip>		
02-Dec-2024	5.5	CVE ID : CVE-2024-53116In the Linux kernel, the following vulnerability has been resolved:virtio/vsock: Improve MSG_ZEROCOPY error handlingAdd a missing kfree_skb() to prevent memory leaks.CVE ID : CVE-2024-53117	https:// git.kerne l.org/sta ble/c/5 0061d7 319e211 65d04e3 024354c 1b43b6 137821, https:// git.kerne l.org/sta ble/c/6 0cf6206 a1f5135 12f5d73 fa4d3db bcad2e7 dcd6	O-LIN-LINU- 241224/1482
02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: vsock: Fix sk_error_queue memory leak	https:// git.kerne l.org/sta ble/c/be a4779a4 5f49275 b1e1b1b d9de03c d37272	O-LIN-LINU- 241224/1483
	02-Dec-2024	02-Dec-2024 5.5 02-Dec-2024 5.5	outpc: panthor_vm_unmap_pages+ 0x124/0x1c8 [panthor] Ir: panthor_vm_unmap_pages+ 0x124/0x1c8 [panthor] <snip> panthor : [drm] *ERROR* failed to unmap range ffffa3886000-ffffa3890000) (requested range ffffa388c000-ffffa3890000) CVE ID : CVE-2024-5311602-Dec-20245.5In the Linux kernel, the following vulnerability has been resolved: Virtio/vsock: Improve MSG_ZEROCOPY error handling02-Dec-20245.5In the Linux kernel, the following vulnerability has been resolved: Virtio/vsock: Improve MSG_ZEROCOPY error handling02-Dec-20245.5In the Linux kernel, the following vulnerability has been resolved: Virtio/vsock: Improve MSG_ZEROCOPY error handling02-Dec-20245.5In the Linux kernel, the following vulnerability has been resolved:</snip>	02-Dec-20245.5pc: panthor_vm_unmap_pages+ 0x124/0x1c8 [panthor] Ir: panthor_vm_unmap_pages+ 0x124/0x1c8 [panthor] <snip> panthor : [drm] *ERROR* failed to unmap range ffffa3880000-ffffa3890000) (requested range ffffa388c000-ffffa3890000) CVE ID : CVE-2024-53116https:// git.kerne l.org/sta ble/c/5 0061d7 319e211 65d04e302-Dec-20245.55.5In the Linux kernel, the following vulnerability has been resolved: MSG_ZER0C0PY error handlinghttps:// git.kerne l.org/sta ble/c/5 0061d7 319e211 65d04e302-Dec-20245.5In the Linux kernel, the following vulnerability has been resolved: MSG_ZER0C0PY error handlinghttps:// git.kerne l.org/sta ble/c/6 0cf6206 a1f5135 12f5d73 fa4d3db bcad2e702-Dec-20245.5In the Linux kernel, the following vulnerability has been resolved:https:// git.kerne l.org/sta ble/c/6 0cf6206 a1f5135 12f5d73 fa4d3db bcad2e702-Dec-20245.5In the Linux kernel, the following vulnerability has been resolved:https:// git.kerne l.org/sta ble/c/be a4779a4 ysock: Fix sk_error_queue memory leakhttps:// git.kerne l.org/sta ble/c/be</br></br></br></br></br></br></br></br></br></snip>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Kernel queues MSG_ZEROCOPY completion notifications on the error queue. Where they remain, until explicitly recv()ed. To prevent memory leaks, clean up the queue when the socket is destroyed.	44d8, https:// git.kerne l.org/sta ble/c/fb f7085b3 ad1c7cc 067783 4c90f98 5f1b4f7 7a33	
			unreferenced object 0xffff8881028beb00 (size 224):		
			comm "vsock_test", pid 1218, jiffies 4294694897		
			hex dump (first 32 bytes):		
			90 b0 21 17 81 88 ff ff 90 b0 21 17 81 88 ff ff!!		
			00 00 00 00 00 00 00 00 00 00 b0 21 17 81 88 ff ff 		
			backtrace (crc 6c7031ca):		
			[<ffffffff81418ef7>] kmem_cache_alloc_node_no prof+0x2f7/0x370</ffffffff81418ef7>		
			[<ffffffff81d35882>] alloc_skb+0x132/0x180</ffffffff81d35882>		
			[<ffffffff81d2d32b>] sock_omalloc+0x4b/0x80</ffffffff81d2d32b>		
			[<ffffffff81d3a8ae>] msg_zerocopy_realloc+0x9e /0x240</ffffffff81d3a8ae>		
			[<fffffffff81fe5cb2>] virtio_transport_send_pkt_i nfo+0x412/0x4c0</fffffffff81fe5cb2>		
			[<fffffffff81fe6183>] virtio_transport_stream_en queue+0x43/0x50</fffffffff81fe6183>		

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
			[<ffffffff81fe0813>] vsock_connectible_sendmsg +0x373/0x450</ffffffff81fe0813>		
			[<fffffff81d233d5>] sys_sendmsg+0x365/0x 3a0</fffffff81d233d5>		
			[<ffffffff81d246f4>] sys_sendmsg+0x84/0xd0</ffffffff81d246f4>		
			[<ffffffff81d26f47>] sys_sendmsg+0x47/0x80</ffffffff81d26f47>		
			[<ffffffff820d3df3>] do_syscall_64+0x93/0x180</ffffffff820d3df3>		
			[<ffffffff8220012b>] entry_SYSCALL_64_after_hw frame+0x76/0x7e</ffffffff8220012b>		
			CVE ID : CVE-2024-53118		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/2	
			virtio/vsock: Fix accept_queue memory leak	415345 042245 de7601d cc6eafdb	
Missing Release of			As the final stages of socket destruction may be delayed, it is possible	e3a3dcc 9e379, https:// git.kerne	
Memory after Effective Lifetime	02-Dec-2024	5.5	that virtio_transport_recv_listen () will be called after the accept_queue	l.org/sta ble/c/8 97617a4 13e0bf1	O-LIN-LINU- 241224/1484
			has been flushed, but before the SOCK_DONE flag has been set. As a result,	c6380e3 b34b2f2 8f45050 8549,	
			sockets enqueued after the flush would remain unremoved, leading to a	https:// git.kerne l.org/sta	
			memory leak.	ble/c/9 46c7600 fa2207c	
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
			vsock_release	c8d3fbc	
			vsock_release	86a518e c56f98a	
			lock	5813	
			virtio_transport_release		
			virtio_transport_close		
			schedule_delayed_work(clo se_work)		
			sk_shutdown = SHUTDOWN_MASK		
			(!) flush accept_queue		
			release		
			virtio_transport_recv_pkt		
			vsock_find_bound_socket		
			lock		
			if flag(SOCK_DONE) return		
			virtio_transport_recv_listen child		
			= vsock_create_connected		
			(!) vsock_enqueue_accept(child)		
			release		
			close_work		
			lock		
			virtio_transport_do_close		
			set_flag(SOCK_DONE)		
			virtio_transport_remove_so ck		
			vsock_remove_sock		

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
			vsock_remove_bound		
			release		
			Introduce a sk_shutdown		
			check to disallow vsock_enqueue_accept()		
			during		
			socket destruction.		
			unreferenced object		
			0xffff888109e3f800 (size		
			2040):		
			comm "kworker/5:2", pid 371, jiffies 4294940105		
			hex dump (first 32 bytes):		
			00 00 00 00 00 00 00 00		
			00 00 00 00 00 00 00 00		
			28 00 0b 40 00 00 00 00		
			00 00 00 00 00 00 00 00 00		
			(@		
			backtrace (crc 9e5f4e84):		
			[<fffffff81418ff1>]</fffffff81418ff1>		
			kmem_cache_alloc_noprof+ 0x2c1/0x360		
			[<ffffffff81d27aa0>]</ffffffff81d27aa0>		
			sk_prot_alloc+0x30/0x120		
			[<ffffffff81d2b54c>] sk_alloc+0x2c/0x4b0</ffffffff81d2b54c>		
			[<ffffffff81fe049a>]</ffffffff81fe049a>		
			vsock_create.constprop.0+		
			0x2a/0x310		
			[<ffffffff81fe6d6c>] virtio_transport_recv_pkt+0</ffffffff81fe6d6c>		
			x4dc/0x9a0		
			[<ffffffff81fe745d>]</ffffffff81fe745d>		
			vsock_loopback_work+0xfd		
			/0x140		
CVSSv3 Scoring		1-2 2	- 3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

NULL 02-Dec-2024 5.5 In error flow of mix5_tc_ct_entry_add_rule(), in case ct_rule_add() https:// gitkerne e 02-Dec-2024 5.5 In error flow of mix5_tc_tt_entry_add_rule(), in case ct_rule_add() https:// gitkerne BUGL Remember 02-Dec-2024 5.5 In error flow of mix5_tc_tt_entry_add_rule(), in case ct_rule_add() https:// gitkerne BUGL Remember 02-Dec-2024 5.5 In error flow of mix5_tc_tt_entry_add_rule(), in case ct_rule_add() https:// gitkerne BUGL Remember 0000000000010 BUGL Remember Bufc/0c 0-LIN-LINU-241224/1485 BUGL Remember BUGL Remember 0000000000010 Bugs/sta blc/c/6 BUGL Remember 0010:mix5_tc_tt_entry_add 0000000000010 Bugs/sta blc/c/6 BUGL Remember 0010:mix5_tc_tt_entry_add 000000000000000000000000000000000000	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer e02-Dec-20245.55.5In error flow of mix5_tc_ct_entry_add_rule() , in case ct_rule_adt() , in case ct_rule_add() , in case ct_rule_add() <br< td=""><td></td><td></td><td></td><td>process_one_work+0x20c/0</td><td></td><td></td></br<>				process_one_work+0x20c/0		
NULL Pointer Dereference e02-Dec-2024 S.55.5In the Linux kernel, the following vulnerability has been resolved:https:// git.kerne Lorg/sta ble/c/0 6dc488a dc488a ble/c/0 dc488a50410-LIN-LINU- 241224/1485NULL Pointer Dereference e02-Dec-20245.5In error flow of mlx5_tc_tc_tentry_add_rule0 uninitiated. Fix it to use attr which has the needed pointer value.0-LIN-LINU- 241224/1485Burger Pointer Dereference e02-Dec-20245.5In error flow of mlx5_tc_tc_tentry_add_rule0 uninitiated. Fix it to use attr which has the needed pointer value.0-LIN-LINU- 241224/1485Burger BUG: kernel log: 0000000000001100, mittps:// git kerne lorg/sta ble/c/0c dc6168a met/mlx5_tc_tc_entry_add rule+0x2b1/0x2f0 mlx5_tc_ct_entry_add rule+0x2b1/0x2f0 e0-LIN-LINU- 241224/1485				worker_thread+0x1bf/0x3a		
NULL Pointer e02-Dec-20245.5In the Linux kernel, the following vulnerability has been resolved:https:// git.kernel lorg/sta ble/c/0o-LIN-LINU- 241224/1485NULL Pointer e02-Dec-20245.5In error flow of mlx5_tc_t_entry_add_rule() , in case ct_rule_add() uninitiated. Fix it to use attr which has the pointer log:0-LIN-LINU- 241224/1485BUG: kernel NULL pointer dereference, address: 0000000000001100-LIN-LINU- 241224/1485BUG: kernel NULL pointer dereference, address: 000000000000011000.566 10.576BUG: kernel NULL pointer dereference, address: 00000000000001100.5760 10.5762BUG: kernel NULL pointer dereference, address: 000000000000001100.5760 10.5762BUG: kernel NULL pointer dereference, address: 000000000000000001100.508bd 10.5764RIP: 0000000000000001100.308bd 17902e9e 276a0ed col9111						
NULL Pointer Dereference e02-Dec-20245.5In the Linux kernel, the following vulnerability has been resolved:https:// git.kerne l.org/sta ble/c/0 ddc488a 593020NULL Pointer Dereferenc e02-Dec-20245.5In error flow of mlx5_tc_t_entry_add_rule(, in case ct_rule_add() uninitiated. Fix it to uninitiated. Fix it to to git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne callback returns error, l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/0c git.kerne l.org/sta ble/c/6 git.kerne l.org/sta ble/c/6 log/git.kerne l.org/sta ble/c/6 git.kerne l.org/sta ble/c/6						
NULL Pointer e02-Dec-20245.5In the Linux kernel, the following vulnerability has been resolved:https:// git.kerne Lorg/sta ble/c/0 6dc488a 593020NULL Pointer Dereferenc e02-Dec-20245.5In error flow of mlx5_tc_ct_entry_add_rule() , in case ct_rule_ad() callback returns error, uninitiated. Fix it to use attr which has the needed pointer value.https:// git.kerne ble/c/0 d223210NULL Pointer Dereferenc e02-Dec-20245.5Figure 1 sit to uninitiated. Fix it to use attr which has the needed pointer value.0-LIN-LINU- 241224/1485NULL Pointer dereference, address: 000000000000110Org/sta ble/c/6 0f, https:// git.kerne ba35041 1dca736 361ef9a 00.60-LIN-LINU- 241224/1485				ret_from_fork_asm+0x1a/0		
NULL Pointer Dereferenc e02-Dec-20245.5following vulnerability has been resolved:git.kerne Lorg/sta ble/c/0 6dc488a 798557 deref in add rule err flowgit.kerne Lorg/sta ble/c/0 6dc488a 593020 d26006 798557NULL Pointer Dereferenc e02-Dec-20245.5In error flow of mlx5_tc_ct_entry_add_rule() , in case ct_rule_add() callback returns error, zone_rule->attr is used uninitiated. Fix it to use attr which has the needed pointer value.696cfed ble/c/0c ble/c/0c ble/c/0c collN-LINU- 241224/1485NULL Pointer Dereferenc e02-Dec-20245.5Kernel log: NUE-strip is used uninitiated. Fix it to is it to callback returns error, is a strip is it to is a strip is it to is a strip is it to is a strip is it to callback returns error, is a strip is it to is a strip is it is a strip is a strip is it is a strip is it is a strip is it is a strip is a strip is a strip is it is a strip is a				CVE ID : CVE-2024-53119		
NULL Pointer e02-Dec-202402-Dec-2024 In error flow of mlx5_tc_ct_entry_add_rule() , in case ct_rule_add()callback returns error, toninitiated. Fix it tocallback returns error, tone-rule->attr is used uninitiated. Fix it tofor cong/sta tone-rule->attr which has the needed pointer value.ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba35041 tdca736ba45041 tdca736ba4600000000000100 transteneeba47000000000000100 transteneeba47000000000000000000000000000000000000				following vulnerability has	git.kerne l.org/sta ble/c/0	
NULL Pointer Dereferenc02-Dec-20245.5In error flow of mlx5_tc_ct_entry_add_rule() , in case ct_rule_add() callback returns error, zone_rule->attr is used 				,	593020 bd2f006 798557	
NULL Pointer Dereferenc02-Dec-20245.5callback returns error, zone_rule>attr is used uninitiated. Fix it tol.org/sta ble/c/0cO-LIN-LINU- 241224/1485e02-Dec-20245.5use attr which has the 				mlx5_tc_ct_entry_add_rule()	4d8359, https://	
needed pointer value.ba350411dca736361ef9aKernel log:0f,BUG: kernel NULL pointerhttps://dereference, address:git.kerne00000000000110l.org/staBIP:0010:mlx5_tc_ct_entry_add_rule+0x2b1/0x2f07902e9e[mlx5_core]276a0edc09bf11	Pointer Dereferenc	02-Dec-2024	5.5	zone_rule->attr is used	l.org/sta ble/c/0c 7c70ff8b	
Kernel log:0f,BUG: kernel NULL pointerhttps://dereference, address:git.kerne00000000000110l.org/staRIP:030f8bd0010:mlx5_tc_ct_entry_add_7902e9erule+0x2b1/0x2f0276a0ed[mlx5_core]c09bf11	e				ba35041 1dca736	
dereference, address: git.kerne 000000000000110 l.org/sta Ble/c/6 ble/c/6 0010:mlx5_tc_ct_entry_add_ 030f8bd rule+0x2b1/0x2f0 276a0ed [mlx5_core] c09bf11				Kernel log:		
RIP:030f8bd0010:mlx5_tc_ct_entry_add_7902e9erule+0x2b1/0x2f0276a0ed[mlx5_core]c09bf11				dereference, address:	git.kerne l.org/sta	
				0010:mlx5_tc_ct_entry_add_ rule+0x2b1/0x2f0	030f8bd 7902e9e 276a0ed	
CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	CVSSv3 Scoring	Scale <u>0-1</u>	1-2 2	-3 3-4 4-5 5-6	1	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				979e4e2	
			Call Trace:	bc2e	
			<task></task>		
			?_die+0x20/0x70		
			?		
			page_fault_oops+0x150/0x 3e0		
			?		
			exc_page_fault+0x74/0x140		
			? asm_exc_page_fault+0x22/0		
			x30		
			?		
			mlx5_tc_ct_entry_add_rule+ 0x2b1/0x2f0 [mlx5_core]		
			?		
			mlx5_tc_ct_entry_add_rule+ 0x1d5/0x2f0 [mlx5_core]		
			mlx5_tc_ct_block_flow_offlo ad+0xc6a/0xf90 [mlx5_core]		
			?		
			nf_flow_offload_tuple+0xd8 /0x190 [nf_flow_table]		
			nf_flow_offload_tuple+0xd8 /0x190 [nf_flow_table]		
			flow_offload_work_handler+ 0x142/0x320 [nf_flow_table]		
			? finish_task_switch.isra.0+0x 15b/0x2b0		
			process_one_work+0x16c/0 x320		

0-1

1-2

Page **575** of **1137**

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Concurrent Execution with Enserved ConditionImage: Second S	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with (Cace Condition')In the Linux kernel, the following vulnerability has been resolved:https:// git.kerne Lorg/sta been resolved:https:// git.kerne Lorg/sta been resolved:https:// git.kerne Lorg/sta been resolved:https:// git.kerne Lorg/sta been resolved:https:// git.kerne Lorg/sta been resolved:https:// git.kerne Lorg/sta been resolved:https:// git.kerne Lorg/sta been resolved:https:// git.kerne Lorg/sta been resolved:https:// git.kerne Lorg/sta beshordof LIN-LINU- 241224/1486Concurrent Execution using Shared Resource with (Race Condition')0-LIN-LINU- sit.kerne Lorg/sta been resolved:0-LIN-LINU- 241224/14860-LIN-LINU- 241224/1486Condition'i5.5-Lock the FTE, delete it from hardware, set the hardware deletion function to NULL and unlock the FTE.bie/c/9 33ef0d1 33ef0d1 33ef0d1 53e9e60 06e3f30 68d0238 68d02380-LIN-LINU- 241224/1486	weakness			<pre>worker_thread+0x28c/0x3a 0 ?pfx_worker_thread+0x10/ 0x10 kthread+0xb8/0xf0 ?pfx_kthread+0x10/0x10 ret_from_fork+0x2d/0x50 ?pfx_kthread+0x10/0x10</pre>		
Image: constraint of the constra				x30		
Concurrent Execution using Shared Resource with02-Dec-20245.5Form solution solutiongit.kerne lorg/sta ble/c/0 94d1a21 21cee1e 85ab07d 4809dcf b5b9, https:// git.kerne process for deleting FTEs: process for deleting FTEs: solutiongit.kerne solution b5b9, https:// git.kerne bbc/c02-Dec-20245.5-Lock the FTE, delete it from hardware, set the hardware deletion function 53e9e60 condition')0-LIN-LINU- 241224/1486						
	Execution using Shared Resource with Improper Synchroniz ation ('Race	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: fs, lock FTE when checking if active The referenced commits introduced a two-step process for deleting FTEs: - Lock the FTE, delete it from hardware, set the hardware deletion function to NULL and unlock the FTE. - Lock the parent flow group, delete the software copy of the FTE, and	git.kerne l.org/sta ble/c/0 94d1a21 21cee1e 85ab07d 74388f9 4809dcf b5b9, https:// git.kerne l.org/sta ble/c/9 33ef0d1 7f012b6 53e9e60 06e3f50 c8d0238 b5ed, https:// git.kerne l.org/sta	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			However, this approach encounters a race condition if a rule with the same match value is added simultaneously. In this scenario, fs_core may set the hardware deletion function to NULL prematurely,	a314419 930f913 5727e39 d77e662 62d5f7b ef6	
			causing a panic during		
			subsequent rule deletions.		
			To prevent this, ensure the active flag of the FTE is checked under a lock, which will prevent the fs_core layer from attaching		
			a new steering rule to an FTE that is in the process		
			of deletion.		
			[438.967589] MOSHE: 2496 mlx5_del_flow_rules del_hw_func		
			[438.968205][cut here]		
			[438.968654] refcount_t: decrement hit 0; leaking memory.		
			[438.969249] WARNING: CPU: 0 PID: 8957 at lib/refcount.c:31 refcount_warn_saturate+0xf b/0x110		
			[438.970054] Modules linked in: act_mirred cls_flower act_gact sch_ingress openvswitch		

Page 577 of 1137

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
weakiless		003303	nsh mlx5_vdpa vringh vhost_iotlb vdpa mlx5_ib mlx5_core xt_conntrack xt_MASQUERADE nf_conntrack_netlink nfnetlink xt_addrtype iptable_nat nf_nat br_netfilter rpcsec_gss_krb5 auth_rpcgss oid_registry overlay rpcrdma rdma_ucm ib_iser libiscsi scsi_transport_iscsi ib_umad rdma_cm ib_ipoib iw_cm ib_cm ib_uverbs ib_core zram zsmalloc fuse [last unloaded: cls_flower]	Fatch	
			[438.973288] CPU: 0 UID: 0 PID: 8957 Comm: tc Not tainted 6.12.0-rc1+ #8 [438.973888] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0- gf21b5a4aeb02- prebuilt.qemu.org 04/01/2014		
			[438.974874] RIP: 0010:refcount_warn_satura te+0xfb/0x110		
			[438.975363] Code: 40 66 3b 82 c6 05 16 e9 4d 01 01 e8 1f 7c a0 ff 0f 0b c3 cc cc cc cc 48 c7 c7 10 66 3b 82 c6 05 fd e8 4d 01 01 e8 05 7c a0 ff <0f> 0b c3 cc cc cc cc 66 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 90		
			[438.976947] RSP: 0018:ffff888124a53610 EFLAGS: 00010286		
			[438.977446] RAX: 0000000000000000 RBX:		
CVSSv3 Scoring *stands for all v		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
			ffff888119d56de0 RCX: 0000000000000000		
			[438.978090] RDX: ffff88852c828700 RSI: ffff88852c81b3c0 RDI: ffff88852c81b3c0		
			[438.978721] RBP: ffff888120fa0e88 R08: 0000000000000000 R09: ffff888124a534b0		
			[438.979353] R10: 0000000000000001 R11: 0000000000000001 R12: ffff888119d56de0		
			[438.979979] R13: ffff888120fa0ec0 R14: ffff888120fa0ee8 R15: ffff888119d56de0		
			[438.980607] FS: 00007fe6dcc0f800(0000) GS:ffff88852c800000(0000) knlGS:00000000000000000		
			[438.983984] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033		
			[438.984544] CR2: 00000000004275e0 CR3: 0000000186982001 CR4: 000000000372eb0		
			[438.985205] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 00000000000000000		
			[438.985842] DR3: 0000000000000000 DR6: 000000000fffe0ff0 DR7: 00000000000000400		
			[438.986507] Call Trace:		
			[438.986799] <task></task>		

3-4 4-5 5-6

7-8 8-9

9-10

6-7

1-2

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<pre>[438.987070] ?warn+0x7d/0x110 [438.987426] ? refcount_warn_saturate+0xf b/0x110</pre>		
			[438.987877] ? report_bug+0x17d/0x190		
			[438.988261] ? prb_read_valid+0x17/0x20		
			[438.988659] ? handle_bug+0x53/0x90		
			[438.989054] ? exc_invalid_op+0x14/0x70		
			[438.989458] ? asm_exc_invalid_op+0x16/0 x20		
			[438.989883] ? refcount_warn_saturate+0xf b/0x110		
			[438.990348] mlx5_del_flow_rules+0x2f7/ 0x340 [mlx5_core]		
			[438.990932] mlx5_eswitch_del_rule+0x 49/0x170 [mlx5_core]		
			[438.991519] ? mlx5_lag_is_sriov+0x3c/0x5 0 [mlx5_core]		
			[438.992054] ? xas_load+0x9/0xb0		
			[438.992407] mlx5e_tc_rule_unoffload+0x 45/0xe0 [mlx5_core]		
			[438.993037] mlx5e_tc_del_fdb_flow+0x2 a6/0x2e0 [mlx5_core]		
			[438.993623] mlx5e_flow_put+0x29/0x60 [mlx5_core]		
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5 5-6 0	6-7 7-8	8-9 9-10

CVSSv3 Scoring June _____ CVSSv3 Scoring Scale 0-1

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[438.994161] mlx5e_delete_flower+0x261 /0x390 [mlx5_core]		
			[438.994728] tc_setup_cb_destroy+0xb9/ 0x190		
			[438.995150] fl_hw_destroy_filter+0x94/ 0xc0 [cls_flower]		
			[438.995650] fl_change+0x11a4/0x13c0 [cls_flower]		
			[438.996105] tc_new_tfilter+0x347/0xbc0		
			[438.996503] ?		
			truncated		
			CVE ID : CVE-2024-53121		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/2	
Concurrent Execution using			mptcp: cope racing subflow creation in mptcp_rcv_space_adjust	499585 1d58c4a 205ad0f fa7b2f2 1e479a9	
Shared Resource with	02-Dec-2024	5.5	Additional active subflows - i.e. created by the in kernel path	c8527, https:// git.kerne	O-LIN-LINU- 241224/1487
Improper Synchroniz ation			manager - are included into the subflow list before starting the	l.org/sta ble/c/aa d6412c6 3baa39d	211221/110/
('Race Condition')			3whs.	d813e81	
				f16a14d 976b3de	
			A racing recvmsg() spooling	2e8,	
			data received on an already established	https://	
			subflow would	git.kerne l.org/sta	
			unconditionally call	ble/c/ce	

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
			<pre>tcp_cleanup_rbuf() on all the current subflows, potentially hitting a divide by zero error on the newly created ones. Explicitly check that the subflow is in a suitable state before invoking tcp_cleanup_rbuf(). CVE ID : CVE-2024-53122</pre>	7356ae3 5943cc6 494cc69 2e62d51 a734062 b7d	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mptcp: error out earlier on disconnect Eric reported a division by zero splat in the MPTCP protocol: Oops: divide error: 0000 [#1] PREEMPT SMP KASAN PTI CPU: 1 UID: 0 PID: 6094 Comm: syz-executor317 Not tainted 6.12.0-rc5-syzkaller-00291- g05b92660cdfe #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/13/2024	https:// git.kerne l.org/sta ble/c/5 813022 98524e9 d77c4c4 4ff5156 a6cd112 227ae, https:// git.kerne l.org/sta ble/c/9 55388e1 d5d222c 4101c59 6b536d 41b91a8 b212e, https:// git.kerne l.org/sta ble/c/a6 6805c9b 22caf4e 42af7a6 16f6c6b	O-LIN-LINU- 241224/1488

0-1

1-2

2-3 3-4 4-5

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RIP: 0010:tcp_select_window+ 0x5b4/0x1310 net/ipv4/tcp_output.c:3163	83c90d1 010	
			Code: f6 44 01 e3 89 df e8 9b 75 09 f8 44 39 f3 0f 8d 11 ff ff ff e8		
			0d 74 09 f8 45 89 f4 e9 04 ff ff ff e8 00 74 09 f8 44 89 f0 99 <f7> 7c</f7>		
			24 14 41 29 d6 45 89 f4 e9 ec fe ff ff e8 e8 73 09 f8 48 89		
			RSP: 0018:ffffc900041f7930 EFLAGS: 00010293		
			RAX: 0000000000017e67 RBX: 0000000000017e67 RCX: ffffffff8983314b		
			RDX: 0000000000000000 RSI: ffffffff898331b0 RDI: 00000000000000004		
			RBP: 00000000005d6000 R08: 0000000000000004 R09: 0000000000017e67		
			R10: 000000000003e80 R11: 0000000000000000 R12: 000000000003e80		
			R13: ffff888031d9b440 R14: 000000000017e67 R15: 0000000002eb000		
			FS: 00007feb5d7f16c0(0000) GS:ffff8880b8700000(0000		
) knlGS:000000000000000000		
			CS: 0010 DS: 0000 ES: 0000 CR0: 000000080050033		

5-6 6-7 8-9

9-10

7-8

4-5

3-4

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CR2: 00007feb5d8adbb8 CR3: 0000000074e4c000 CR4: 0000000003526f0		
			DR0: 0000000000000000 DR1: 0000000000000000 DR2: 000000000000000000		
			DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 00000000000000400		
			Call Trace:		
			<task></task>		
			tcp_cleanup_rbuf+0x3e7/ 0x4b0 net/ipv4/tcp.c:1493		
			mptcp_rcv_space_adjust net/mptcp/protocol.c:2085 [inline]		
			mptcp_recvmsg+0x2156/0x 2600		
			net/mptcp/protocol.c:2289		
			inet_recvmsg+0x469/0x6a0 net/ipv4/af_inet.c:885		
			sock_recvmsg_nosec net/socket.c:1051 [inline]		
			sock_recvmsg+0x1b2/0x25 0 net/socket.c:1073		
			sys_recvfrom+0x1a5/0x2 e0 net/socket.c:2265		
			do_sys_recvfrom net/socket.c:2283 [inline]		
			se_sys_recvfrom net/socket.c:2279 [inline]		
			x64_sys_recvfrom+0xe0/0 x1c0 net/socket.c:2279		
			do_syscall_x64 arch/x86/entry/common.c: 52 [inline]		

0-1

1-2

2-3

5-6 6-7

8-9

7-8

8-9 9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_syscall_64+0xcd/0x250 arch/x86/entry/common.c: 83		
			entry_SYSCALL_64_after_hw frame+0x77/0x7f		
			RIP: 0033:0x7feb5d857559		
			Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 51 18 00 00 90 48 89 f8 48		
			89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d		
			01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48		
			RSP: 002b:00007feb5d7f1208 EFLAGS: 00000246 ORIG_RAX: 00000000000002d		
			RAX: fffffffffffffffda RBX: 00007feb5d8e1318 RCX: 00007feb5d857559		
			RDX: 000000800000000e RSI: 0000000000000000 RDI: 0000000000000003		
			RBP: 00007feb5d8e1310 R08: 0000000000000000 R09: ffffffff81000000		
			R10: 0000000000000100 R11: 000000000000246 R12: 00007feb5d8e131c		
			R13: 00007feb5d8ae074 R14: 000000800000000e R15: 00000000fffffdef		
			and provided a nice reproducer.		

0-1

1-2

2-3

Page 585 of 1137

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The root cause is the current bad handling of racing disconnect.		
			After the blamed commit below, sk_wait_data() can return (with		
			error) with the underlying socket disconnected and a zero rcv_mss.		
			Catch the error and return without performing any additional		
			operations on the current socket.		
			CVE ID : CVE-2024-53123		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne	
			drm/xe/oa: Fix "Missing outer runtime PM protection" warning	l.org/sta ble/c/c0 403e4ce ecaefbea	
NY / A			Fix the following drm_WARN:	f78263d ffcd3e3f 06a19f6 b,	O-LIN-LINU-
N/A	04-Dec-2024	5.5	[953.586396] xe 0000:00:02.0: [drm] Missing outer runtime PM protection 	https:// git.kerne l.org/sta ble/c/ed 7cd3510 d8da6e3	241224/1489
			<4> [953.587090] ? xe_pm_runtime_get_noresu me+0x8d/0xa0 [xe]	578d91 25a9ea4 440f8ad	
			<4> [953.587208] guc_exec_queue_add_msg+0 x28/0x130 [xe]	eeaa	

0-1

1-2

Page **586** of **1137**

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<4> [953.587319] guc_exec_queue_fini+0x3a/ 0x40 [xe]		
			<4> [953.587425] xe_exec_queue_destroy+0xb 3/0xf0 [xe]		
			<4> [953.587515] xe_oa_release+0x9c/0xc0 [xe]		
			(cherry picked from commit b107c63d2953907908fd0c afb0e543b3c3167b75)		
			CVE ID : CVE-2024-53132		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/2	
			pmdomain: imx93-blk-ctrl: correct remove path	01fb9e1 64a1e4c 5937de2 cf58bcb	
Always-			The check condition should be 'i < bc- >onecell_data.num_domains ', not	0327c08 664f, https:// git.kerne	
Incorrect Control Flow Implement ation	04-Dec-2024	5.5	'bc- >onecell_data.num_domains ' which will make the look never finish	l.org/sta ble/c/8f c228ab5 d38a026 eae7183	O-LIN-LINU- 241224/1490
			and cause kernel panic.	a5f74a4f ac43d9b	
			Also disable runtime to address	6a, https:// git.kerne	
			"imx93-blk-ctrl 4ac10000.system-	l.org/sta ble/c/f7 c7c5aa5	
			controller: Unbalanced pm_runtime_enable!"	56378a2	
			CVE ID : CVE-2024-53134	c8da72c 1f7f238	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				b6648f9 5fb	
N/A	04-Dec-2024	04-Dec-2024 05.5 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	following vulnerability has been resolved: ARM: fix cacheflush with PAN It seems that the cacheflush	https:// git.kerne l.org/sta ble/c/ca 29cfcc4a 21083d 671522a d38453 2e28a43 f033, https://	0-LIN-LINU- 241224/1491
			git.kerne l.org/sta ble/c/e6 960a2ed 49c9a25 357817 535f7cc 50594a5	241224/1491	
			In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: kTLS, Fix incorrect page refcounting	https:// git.kerne l.org/sta ble/c/2 723e8b2 cbd486c b96e5a6	
N/A CVSSv3 Scoring	04-Dec-2024	5.5	The kTLS tx handling code is using a mix of get_page() and page_ref_inc() APIs to increment the page reference. But on the release path (mlx5e_ktls_tx_handle_resy nc_dump_comp()), only put_page() is used.	1b2247 3f7fd62 e18df, https:// git.kerne l.org/sta ble/c/6 9fbd07f 17b0fda f8970bc 705f5bf 115c297 839d, https://	O-LIN-LINU- 241224/1492 8-9 9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This is an issue when using pages from large folios: the get_page() references are stored on the folio page while the page_ref_inc() references are stored directly in the given page. On release the folio	git.kerne l.org/sta ble/c/9 3a14620 b97c911 489a5b0 08782f3 d9b0c4a eff4	
			page will be dereferenced too many times.		
			This was found while doing kTLS testing with sendfile() + ZC when the		
			served file was read from NFS on a kernel with NFS large folios support		
			(commit 49b29a573da8 ("nfs: add support for large folios")).		
			CVE ID : CVE-2024-53138		
Concurrent Execution using Shared			In the Linux kernel, the following vulnerability has been resolved: net: fix data-races around sk->sk_forward_alloc	https:// git.kerne l.org/sta ble/c/0 73d898 08c065a c4c672c	
Resource with Improper Synchroniz ation ('Race	02-Dec-2024	4.7	Syzkaller reported this warning: [cut here] WARNING: CPU: 0 PID: 16	0a613a7 1b27a80 691cb, https:// git.kerne l.org/sta	O-LIN-LINU- 241224/1493
Condition')			at net/ipv4/af_inet.c:156 inet_sock_destruct+0x1c5/0 x1e0 Modules linked in:	ble/c/d 285eb9d 0641c83 44f2836 081b4cc	

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
			CPU: 0 UID: 0 PID: 16 Comm: ksoftirqd/0 Not tainted 6.12.0-rc5 #26	b7b3c5c c1b6	
			Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014		
			RIP: 0010:inet_sock_destruct+0x 1c5/0x1e0		
			Code: 24 12 4c 89 e2 5b 48 c7 c7 98 ec bb 82 41 5c e9 d1 18 17 ff 4c 89 e6 5b 48 c7 c7 d0 ec bb 82 41 5c e9 bf 18 17 ff 0f 0b eb 83 <0f> 0b eb 97 0f 0b eb 87 0f 0b e9 68 ff ff ff 66 66 2e 0f 1f 84 00		
			RSP: 0018:ffffc9000008bd90 EFLAGS: 00010206		
			RAX: 0000000000000300 RBX: ffff88810b172a90 RCX: 0000000000000007		
			RDX: 0000000000000002 RSI: 000000000000300 RDI: ffff88810b172a00		
			RBP: ffff88810b172a00 R08: ffff888104273c00 R09: 0000000000100007		
			R10: 0000000000020000 R11: 0000000000000006 R12: ffff88810b172a00		
			R13: 00000000000000004 R14: 00000000000000000 R15: ffff888237c31f78		
			FS: 0000000000000000000000000000 GS:ffff888237c00000(0000) knlGS:000000000000000000		

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CS: 0010 DS: 0000 ES:		
			0000 CR0: 0000000080050033		
			CR2: 00007ffc63fecac8		
			CR3: 00000000342e000		
			CR4: 00000000000006f0		
			DR0: 00000000000000000 DR1: 000000000000000000		
			DR2: 000000000000000000000000000000000000		
			DR3: 000000000000000000		
			DR6: 00000000fffe0ff0 DR7: 00000000000000400		
			Call Trace:		
			<task></task>		
			<143K> ?_warn+0x88/0x130		
			?		
			inet_sock_destruct+0x1c5/0		
			x1e0		
			?		
			report_bug+0x18e/0x1a0		
			? handle_bug+0x53/0x90 ?		
			? exc_invalid_op+0x18/0x70		
			?		
			asm_exc_invalid_op+0x1a/0		
			x20		
			? inet_sock_destruct+0x1c5/0		
			x1e0		
			_sk_destruct+0x2a/0x200		
			rcu_do_batch+0x1aa/0x530		
			? rcu_do_batch+0x13b/0x530		
			rcu_core+0x159/0x2f0		
			104_016 (08137/08210		
			handle_softirqs+0xd3/0x2b		
			0		
CVSSv3 Scoring	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? pfx_smpboot_thread_fn+0 x10/0x10 run_ksoftirqd+0x25/0x30		
			<pre>smpboot_thread_fn+0xdd/0 x1d0 kthread+0xd3/0x100 ?pfx_kthread+0x10/0x10 ret_from_fork+0x34/0x50</pre>		
			? pfx_kthread+0x10/0x10		
			ret_from_fork_asm+0x1a/0 x30 [end trace 000000000000000]		
			Its possible that two threads call tcp_v6_do_rcv()/sk_forward _alloc_add() concurrently when sk- >sk_state == TCP_LISTEN		
			with sk->sk_lock unlocked, which triggers a data-race around sk- >sk_forward_alloc:		
			tcp_v6_rcv tcp_v6_do_rcv skb_clone_and_charge_r		
			sk_rmem_schedule sk_mem_schedule		
			sk_forward_alloc_add()		

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			skb_set_owner_r		
			sk_mem_charge		
			sk_forward_alloc_add()		
			kfree_skb		
			skb_release_all		
			Shb_i cicube_un		
			skb_release_head_state		
			sock_rfree		
			sk_mem_uncharge		
			sk_forward_alloc_add()		
			sk_mem_reclaim		
			// set local var reclaimable		
			sk_mem_reclaim		
			sk_forward_alloc_add()		
			In this syzkaller testcase, two threads call		
			tcp_v6_do_rcv() with skb- >truesize=768, the sk_forward_alloc changes like		
			this:		
			(cpu 1) (cpu 2) sk_forward_alloc		
			0		
			sk_mem_schedule()		
			+4096 = 4096		
			 sk_mem_schedule() +4096 = 8192		
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	Description & CVE ID sk_mem_charge() -768 = 7424 sk_mem_charge() -768 = 6656 sk_mem_uncharge() +768 = 7424 reclaimable=7424 sk_mem_uncharge() +768 = 8192 reclaimable=8192 sk_mem_reclaim()	Patch	NCIIPC ID
			-4096 = 4096 sk_mem_reclaim() -8192 = -4096 != 0		
			The skb_clone_and_charge_r() should not be called in tcp_v6_do_rcv() when		
			sk->sk_state is TCP_LISTEN, it happens later in tcp_v6_syn_recv_sock().		
			Fix the same issue in dccp_v6_do_rcv(). CVE ID : CVE-2024-53124		
Affected Vers	sion(s): From (i	ncluding)	2.6.12 Up to (excluding) 4.19.3	325	
Out-of- bounds Write	06-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: initramfs: avoid filename buffer overrun	https:// git.kerne l.org/sta ble/c/1a 423bbbe af9e3e2 0c46865	O-LIN-LINU- 241224/1494
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
			The initramfs filename field is defined in Documentation/driver- api/early-userspace/buffer- format.rst as:	01efd9b 661fe83 4db, https:// git.kerne l.org/sta ble/c/4 9d01e73	
			37 cpio_file := ALGN(4) + cpio_header + filename + "\0" + ALGN(4) + data 55 ================================	6c30453 19e030d 1e75fb9 83011ab aca7, https:// git.kerne	
			====== 56 Field name Field size Meaning 57 ====================================	l.org/sta ble/c/bb 7ac9667 0ab1d8d 681015f 9d66e45 dad579a f4d	
			==== 70 c_namesize 8 bytes Length of filename, including final \0		
			When extracting an initramfs cpio archive, the kernel's do_name() path handler assumes a zero- terminated path at @collected, passing it directly to file_open() /		
			directly to filp_open() / init_mkdir() / init_mknod(). If a specially crafted cpio entry carries a non-zero- terminated filename		

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
			and is followed by uninitialized memory, then a file may be created with		
			trailing characters that represent the uninitialized memory. The ability		
			to create an initramfs entry would imply already having full control of		
			the system, so the buffer overrun shouldn't be considered a security		
			vulnerability.		
			Append the output of the following bash script to an existing initramfs		
			and observe any created /initramfs_test_fname_over runAA* path. E.g.		
			./reproducer.sh gzip >> /myinitramfs		
			It's easiest to observe non- zero uninitialized memory when the output is		
			gzipped, as it'll overflow the heap allocated @out_buf in gunzip(),		
			rather than the initrd_start+initrd_size block.		
			reproducer.sh		
			nilchar="A" # change to "\0" to properly zero terminate / pad		
			magic="070701"		

0-1

1-2

2-3

Page **596** of **1137**

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Descrij	otion & C	/E ID	P	atch	NCIIP	CID
			ino=1						
			mode=\$((0100777))				
			uid=0						
			gid=0						
			nlink=1						
			mtime=1						
			filesize=0						
			devmajor=	0					
			devminor=	1					
			rdevmajor	=0					
			rdevminor	=0					
			csum=0						
			fname="ini e_overrun"		est_fnan	n			
			namelen=\$)) # pl account for	us one to	D				
			printf "%s%08x% %08x%08 x%08x%08 " \	x%08x%	08x%08	3			
			\$ma \$uid \$gid \$ \$filesize \	agic \$ino nlink \$m					
			\$de \$devminor \$rdevmino \$csum \$fna	r \$name	•				
			termpadler ((110 + \$n; 4))) printf "%.s	amelen)	& 3)) %				
			1 \$termpao		-	-			
			reprod	ucer.sh -					
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
			Symlink filename fields handled in do_symlink() won't overrun past the		
			data segment, due to the explicit zero-termination of the symlink		
			target.		
			Fix filename buffer overrun by aborting the initramfs FSM if any cpio		
			entry doesn't carry a zero- terminator at the expected (name_len - 1)		
			offset.		
			CVE ID : CVE-2024-53142		
Affected Ver	sion(s): From (i	ncluding)	2.6.25 Up to (excluding) 4.19.3	1	
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/6	
			ocfs2: uncache inode which has failed entering the group	20d225 98110b 0d0cb97 a3fcca65 fc473ea	
N/A	02-Dec-2024	5.5	Syzbot has reported the following BUG:	86e73, https:// git.kerne l.org/sta	O-LIN-LINU- 241224/1495
			kernel BUG at fs/ocfs2/uptodate.c:509! 	ble/c/7 37f3413 7844d6 572ab7d	
			Call Trace:	473c998	
			<task></task>	c7f977ff 30eb,	
			?die_body+0x5f/0xb0	https://	
			? die+0x9e/0xc0	git.kerne l.org/sta	
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
Weakness	Publish Date	CVSSv3	? do_trap+0x15a/0x3a0 ? ocfs2_set_new_buffer_uptod ate+0x145/0x160 ? do_error_trap+0x1dc/0x2c 0 ? ocfs2_set_new_buffer_uptod ate+0x145/0x160 ? pfx_do_error_trap+0x10/0 x10 ? handle_invalid_op+0x34/0x 40 ? ocfs2_set_new_buffer_uptod ate+0x145/0x160 ? exc_invalid_op+0x38/0x50 ? asm_exc_invalid_op+0x1a/0 x20 ? ocfs2_set_new_buffer_uptod ate+0x2e/0x160 ? ocfs2_set_new_buffer_uptod ate+0x144/0x160 ?	Patch ble/c/8 43dfc80 4af4b33 8ead423 31dd58 081b42 8ecdf8	
			ocfs2_group_add+0x39f/0x 15a0 ? pfx_ocfs2_group_add+0x1 0/0x10		

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? pfx_lock_acquire+0x10/0x 10		
			? mnt_get_write_access+0x68 /0x2b0		
			? pfx_lock_release+0x10/0x 10		
			? rcu_read_lock_any_held+0x b7/0x160		
			? pfx_rcu_read_lock_any_hel d+0x10/0x10		
			? smack_log+0x123/0x540 ?		
			mnt_get_write_access+0x68 /0x2b0 ?		
			mnt_get_write_access+0x68 /0x2b0 ?		
			mnt_get_write_access+0x22 6/0x2b0		
			ocfs2_ioctl+0x65e/0x7d0 ? pfx_ocfs2_ioctl+0x10/0x1		
			0 ? smack_file_ioctl+0x29e/0x3		
			a0 ?		
			pfx_smack_file_ioctl+0x10 /0x10 ?		
			lockdep_hardirqs_on_prepa re+0x43d/0x780		

3-4 4-5 5-6

7-8 8-9 9-10

6-7

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? pfx_lockdep_hardirqs_on_ prepare+0x10/0x10 ?		
			pfx_ocfs2_ioctl+0x10/0x1 0		
			se_sys_ioctl+0xfb/0x170		
			do_syscall_64+0xf3/0x230		
			entry_SYSCALL_64_after_hw frame+0x77/0x7f		
			When 'ioctl(OCFS2_IOC_GROUP_A DD,)' has failed for the particular		
			inode in 'ocfs2_verify_group_and_inp ut()', corresponding buffer head		
			remains cached and subsequent call to the same 'ioctl()' for the same		
			inode issues the BUG() in 'ocfs2_set_new_buffer_upto date()' (trying		
			to cache the same buffer head of that inode). Fix this by uncaching		
			the buffer head with 'ocfs2_remove_from_cache()' on error path in		
			'ocfs2_group_add()'.		
			CVE ID : CVE-2024-53112		
Affected Ver	sion(s): From (i	ncluding)	2.6.39 Up to (excluding) 4.19.3	325	

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
	N/A 06-Dec-2024 7.8		In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: add missing range check in bitmap_ip_uadt	https:// git.kerne l.org/sta ble/c/1 579483 5378ed5 6fb9bac c6a5dd3 b9f3352 0604e,	
N/A		06-Dec-2024 7.8	5-Dec-2024 7.8	When tb[IPSET_ATTR_IP_TO] is not present but tb[IPSET_ATTR_CIDR] exists, the values of ip and ip_to are slightly swapped. Therefore, the range check	https:// git.kerne l.org/sta ble/c/3 5f56c55 4eb1b56 b77b3cf 197a6b0 0922d4
			for ip should be done later, but this part is missing and it seems that the vulnerability occurs. So we should add missing range checks and remove unnecessary range checks.	9033d, https:// git.kerne l.org/sta ble/c/3c 20b594 8f119ae 61ee35a d8584d	
			CVE ID : CVE-2024-53141	666020c 91581	
Affected Ver	sion(s): From (i	ncluding)	3.9 Up to (excluding) 6.1.119		
NULL			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/2 026559a	
Pointer Dereferenc e	04-Dec-2024	5.5	nilfs2: fix null-ptr-deref in block_dirty_buffer tracepoint	6c4ce34 db117d 2db8f71 0fe2a94 20d5a,	O-LIN-LINU- 241224/1497
			When using the "block:block_dirty_buffer"	https:// git.kerne	

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tracepoint, mark_buffer_dirty() may cause a NULL pointer dereference, or a general protection fault when KASAN is enabled.	l.org/sta ble/c/7a f3309c7 a2ef268 31a6712 5b11c34 a7e01c1 b2a,	
			This happens because, since the tracepoint was added in mark_buffer_dirty(), it references the dev_t member bh->b_bdev- >bd_dev	https:// git.kerne l.org/sta ble/c/8 6b1903 1dbc79a bc378df	
			regardless of whether the buffer head has a pointer to a block_device structure.	ae357f6 ea33ebe b0c95	
			In the current implementation, nilfs_grab_buffer(), which grabs a buffer		
			to read (or create) a block of metadata, including b- tree node blocks,		
			does not set the block device, but instead does so only if the buffer is		
			not in the "uptodate" state for each of its caller block reading		
			functions. However, if the uptodate flag is set on a folio/page, and the		
			buffer heads are detached from it by try_to_free_buffers(), and new buffer		

0-1

1-2

2-3

3-4 4-5 5-6

9-10

NULL 04-Dec-2024 5.5 In the Linux kernel, the following vulnerability has beer restored to generation block device being set to bh->b, bdev, and mark, buffer, dirty() may be called later in that state, resulting in the bug mentioned above. Fix this issue by making nilfs_grab_buffer() always set the block device of the super block structure to the buffer head, regardless of the state of the buffer's uptodate flag. CVE ID : CVE-2024-53130 NULL Pix the instructure following vulnerability has been resolved: https:// Patch series "nilfs2: fix null-ptr-deref in block_touch_buffer 04-Dec-2024 5.5 Patch series "nilfs2: fix null-ptr-deref in block_touch_buffer 04-Dec-2024 5.5 Patch series "nilfs2: fix null-ptr-deref in block_touch_buffer 04-Dec-2024 5.5 Patch series "nilfs2: fix null-ptr-deref in block_touch_buffer 04-Dec-2024 5.5 Vibra Scotege and the using nilfs2 and two block-related a05a0c0 0-LIN-LINU-241224/1498 Vibra Scotege and the using nilfs2 and two block-related a05a0c0 a05a0c0 NULL Provide and the using nilfs2 and two block-related a05a0c0 a05a0c0 Vibra Scotege and the using nilfs2 and two block-related a05a0c0 a05a0c0 Attace and two block-related a05a0c0 a05a0c0 Bible And two block-related a05a0c0 a05a0c0 Bible And two block-related a04boc a05a0c0 <	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer e0.4-Dec-20245.55.511 <td></td> <td></td> <td></td> <td>create_empty_buffers(), the</td> <td></td> <td></td>				create_empty_buffers(), the		
NULL Pointer e04-Dec-20245.55.5Fix this series fixes null pointer block_touch_buffer inits_grand_tout out out out out out out out out out				without the block device		
NULL Pointer e04-Dec-20245.55.5Fix this issue by making nilfs_grab_buffer() always set the block device of the super block structure to the buffer head, regardless of the state of the buffer's uptodate flag. CVE ID : CVE-2024-53130https:// git.kerne lorg/sta ble/c/0https:// git.kerne lorg/sta ble/c/0NULL Pointer e04-Dec-20245.5Patch series "nilfs2: fix null-ptr-deref in block_touch_buffer tracepoints".https:// git.kerne lorg/sta ble/c/00-LIN-LINU- lorg/sta ble/c/0NULL Pointer e04-Dec-20245.5Patch series "nilfs2: fix null- ptr-deref bugs on block tracepoints".0-LIN-LINU- lorg/sta ble/c/3 loid a05a0c0 loid a05a0c0 loid a05a0c0 loid a05a0c0 loid a05a0c00-LIN-LINU- loid a05a0c0 loid a05a0c0 loid a05a0c0 loid a05a0c0				mark_buffer_dirty() may be		
NULL Pointer e04-Dec-20245.55.5In the Linux kernel, the following vulnerability has been resolved:https:// git.kerne block_touch_buffer yege02er04-Dec-20245.5In the Linux kernel, the following vulnerability has been resolved:https:// git.kerne block_touch_buffer yege02er04-Dec-20245.5Patch series "nilfs2: fix null-ptr-deref in block_touch_buffer tracepointb8bf. git.kerne block_touch_buffer yege02er yege02er git.kerne block_touch_buffer tracepoint04-Dec-20245.5Patch series "nilfs2: fix null-ptr-deref in block_touch_buffer tracepoints04-Dec-20245.5Patch series "nilfs2: fix null-ptr-deref in block_touch_buffer tracepoints04-Dec-202404-D						
NULL Pointer e04-Dec-20245.55.55.55.5For the series "nilfs2: fix null-ptr-deref hugs on block tracepoints".NULL Pointer infs2: fix null-ptr-deref in block_touch_buffer tracepointsNULL Pointer infs2: fix null-ptr-deref in block_touch_buffer tracepoints0.111111111111111111111111111111111111				nilfs_grab_buffer() always		
NULL Pointer Dereferenc04-Dec-20245.55.5In the Linux kernel, the following vulnerability has been resolved:https:// git.kerne Lorg/sta ble/c/00-LIN-LINU- 241224/1498NULL Pointer Dereferenc e04-Dec-20245.5Patch series "nilfs2: fix null- ptr-deref bugs on block tracepoints".0-LIN-LINU- 241224/1498NULL Pointer Dereferenc e04-Dec-20245.5Patch series "nilfs2: fix null- ptr-deref bugs on block tracepoints".0-LIN-LINU- 241224/1498				to the buffer head,		
NULL Pointer Dereference e04-Dec-20245.5In the Linux kernel, the following vulnerability has been resolved:NULL Pointer 100098556b1 8556b1 8670e26NULL Pointer Dereference e04-Dec-20245.594th series "nilfs2: fix null-ptr-deref in block_touch_buffer tracepoint88bf, 10100-LIN-LINU- 241224/1498NULL Pointer Dereference e04-Dec-20245.594th series "nilfs2: fix null- ptr-deref bugs on block tracepoints".88bf, 10160080-LIN-LINU- 241224/1498NULL Patch series "nilfs2: fix null- ptr-deref bugs on block tracepoints".104c07 101620-LIN-LINU- 241224/1498NULL ptr-deref bugs on block tracepoints".104c07 101620-LIN-LINU- 241224/1498NULL ptr-deref bugs on block tracepoints".104c07 101620-LIN-LINU- 241224/1498NULL ptr-deref bugs on block tracepoints.104c07 104c070-LIN-LINU- 241224/1498				of the buffer's uptodate flag.		
NULL Pointer e04-Dec-20245.5following vulnerability has been resolved:git.kern Lorg/sta ble/(/0NULL Pointer Dereference e04-Dec-20245.5Fach series "nilfs2: fix null-ptr-deref in block_touch_buffer tracepoint85556bf 8670e26Patch series "nilfs2: fix null- ptr-deref bugs on block tracepoints".8b8f, b8bf, 1016a08Image: Dereference e04-Dec-20245.5Patch series "nilfs2: fix null- ptr-deref bugs on block tracepoints".9268dac b8bf, b8bf, b16/c/3Image: Dereference ptr-deref bugs on block tracepoints".04-Dec-2024Image: Dereference block tracepoints101Image: Dereference block tracepoints102Image: Dereferen				CVE ID : CVE-2024-53130		
NULL 04-Dec-2024 5.5 nilfs2: fix null-ptr-deref in block_touch_buffer tracepoint 8556bf 8c70e26 20000 9268dac 3016000 Dereferenc 04-Dec-2024 5.5 Patch series "nilfs2: fix null-ptr-deref bugs on block tracepoints". 88bf. 0-LIN-LINU- Dereference 101 1007/sta<10000				following vulnerability has	git.kerne l.org/sta	
NOLL 04-Dec-2024 5.5 Patch series "nilfs2: fix null- ptr-deref bugs on block tracepoints". b8bf, 0-LIN-LINU- 241224/1498 e 1.org/sta ble/c/3 ble/c/3 ble/c/3 5.5 This series fixes null pointer blee77a ble/c/3 blee77a blee77a ofd3ed5 nilfs2 and two block-related a05a0c0 2b6cde8 nilfs2 and two block-related bd9, bley. 1.org/sta blee77a bley. bley. bley. bley. bley. bley.				block_touch_buffer	8c70e26 29e02e7 9268dac	
This series fixes null pointerb2a4fd9dereference bugs that occurbbee77awhen usingfdd3ed5nilfs2 and two block-related tracepoints.a05a0c02b6cde8d3b9,https://	Pointer Dereferenc	04-Dec-2024	5.5	ptr-deref bugs on block	b8bf, https:// git.kerne l.org/sta	
tracepoints. 2b6cde8 d3b9, https://				dereference bugs that occur when using	b2a4fd9 bbee77a fdd3ed5	
CVSSv3 Scoring Scale 0-1 1-2 -2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10					2b6cde8 d3b9,	
	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
			This patch (of 2):	git.kerne l.org/sta ble/c/5 9b49ca6	
			It has been reported that when using "block:block_touch_buffer"	7cca7b0 07a5afd 3de0283	
			tracepoint, touch_buffer() called from nilfs_get_folio_block() causes a	c800815 7665	
			NULL pointer dereference, or a general protection fault when KASAN is		
			enabled.		
			This happens because since the tracepoint was added in touch_buffer(), it		
			references the dev_t member bh->b_bdev- >bd_dev regardless of whether the		
			buffer head has a pointer to a block_device structure. In the current		
			implementation, the block_device structure is set after the function		
			returns to the caller.		
			Here, touch_buffer() is used to mark the folio/page that owns the buffer		
			head as accessed, but the common search helper for folio/page used by the		
			caller function was optimized to mark the		

0-1

1-2

2-3

Page **605** of **1137**

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			folio/page as accessed when it		
			was reimplemented a long time ago, eliminating the need to call		
			touch_buffer() here in the first place.		
			So this solves the issue by eliminating the touch_buffer() call itself.		
			CVE ID : CVE-2024-53131		
Affected Ver	sion(s): From (i	ncluding)	4.19.322 Up to (excluding) 4.2	20	
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/0	
			Revert "mmc: dw_mmc: Fix IDMAC operation with pages bigger than 4K"	0bff717 45bc358 3bd5ca5 9be91e0 ee1d27f	
			The commit 8396c793ffdf ("mmc: dw_mmc: Fix IDMAC operation with pages	1944, https:// git.kerne l.org/sta	
N/A	04-Dec-2024	5.5	bigger than 4K") increased the max_req_size, even for 4K pages, causing	ble/c/1 635e407 a4a64d0 8a8517a	O-LIN-LINU- 241224/1499
			various issues:	c59ca14	
			- Panic booting the kernel/rootfs from an SD card on Rockchip RK3566	ad4fc78 5e75, https://	
			- Panic booting the kernel/rootfs from an SD card on StarFive JH7100	git.kerne l.org/sta ble/c/5 6de724c	
			- "swiotlb buffer is full" and data corruption on StarFive JH7110	58c07a7 ca3aac0 27cfd2c	

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
			At this stage no fix have been found, so it's probably better to just revert the change. This reverts commit 8396c793ffdf28bb8aee7cfe 0891080f8cab7890.	cb184ed 9e4e	
			CVE ID : CVE-2024-53127		
Affected Ver	<mark>sion(s): From (</mark> i	ncluding)	4.19.323 Up to (excluding) 4.1	9.325	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	04-Dec-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: mm: revert "mm: shmem: fix data-race in shmem_getattr()" Revert d949d1d14fa2 ("mm: shmem: fix data-race in shmem_getattr()") as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over NFS. As Hugh commented, "added just to silence a syzbot sanitizer splat: added where there has never been any practical problem". CVE ID : CVE-2024-53136	https:// git.kerne l.org/sta ble/c/3 6b537e8 f302f67 0c7cf35 d88a3a2 94443e3 2d52, https:// git.kerne l.org/sta ble/c/5 874c115 0e77296 565ad6e 495ef41 fbf8757 0d14, https:// git.kerne l.org/sta ble/c/6 4e67e86 94252c1 bf01b80 2ee911b e3fee62 c36b	O-LIN-LINU- 241224/1500

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Affected Ver	Affected Version(s): From (including) 4.20 Up to (excluding) 6.1.119								
			4.20 Up to (excluding) 6.1.119 In the Linux kernel, the following vulnerability has been resolved: ocfs2: uncache inode which has failed entering the group Syzbot has reported the following BUG: kernel BUG at fs/ocfs2/uptodate.c:509! Call Trace: <task> ?die_body+0x5f/0xb0 ? die+0x9e/0xc0 ? do_trap+0x15a/0x3a0 ? ocfs2_set_new_buffer_uptod</task>	https:// git.kerne l.org/sta ble/c/6 20d225 98110b 0d0cb97 a3fcca65 fc473ea 86e73, https:// git.kerne l.org/sta ble/c/7 37f3413 7844d6 572ab7d 473c998 c7f977ff 30eb, https://	NCIIPC ID				
			https:// git.kerne l.org/sta ble/c/8 43dfc80 4af4b33 8ead423 31dd58						
			? pfx_do_error_trap+0x10/0 x10 ? handle_invalid_op+0x34/0x 40	081b42 8ecdf8					

4-5 5-6

6-7

7-8

8-9

9-10

2-3

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? ocfs2_set_new_buffer_uptod ate+0x145/0x160 ? exc_invalid_op+0x38/0x50		
			? asm_exc_invalid_op+0x1a/0 x20 ? ocfs2_set_new_buffer_uptod		
			ate+0x2e/0x160 ? ocfs2_set_new_buffer_uptod ate+0x144/0x160 ?		
			ocfs2_set_new_buffer_uptod ate+0x145/0x160 ocfs2_group_add+0x39f/0x 15a0		
			? pfx_ocfs2_group_add+0x1 0/0x10 ?		
			pfx_lock_acquire+0x10/0x 10 ? mnt_get_write_access+0x68 /0x2b0		
			? pfx_lock_release+0x10/0x 10 ?		
			rcu_read_lock_any_held+0x b7/0x160 ? pfx_rcu_read_lock_any_hel d+0x10/0x10		
			? smack_log+0x123/0x540		

Page **609** of **1137**

4-5

5-6

6-7

7-8

8-9

9-10

3-4

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? mnt_get_write_access+0x68 /0x2b0		
			? mnt_get_write_access+0x68 /0x2b0		
			? mnt_get_write_access+0x22 6/0x2b0		
			ocfs2_ioctl+0x65e/0x7d0 ?		
			pfx_ocfs2_ioctl+0x10/0x1 0		
			? smack_file_ioctl+0x29e/0x3 a0		
			? pfx_smack_file_ioctl+0x10 /0x10		
			? lockdep_hardirqs_on_prepa re+0x43d/0x780		
			? pfx_lockdep_hardirqs_on_ prepare+0x10/0x10		
			? pfx_ocfs2_ioctl+0x10/0x1 0		
			se_sys_ioctl+0xfb/0x170 do_syscall_64+0xf3/0x230		
			entry_SYSCALL_64_after_hw		
			frame+0x77/0x7f		
			When 'ioctl(OCFS2_IOC_GROUP_A		

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
			DD,)' has failed for the particular inode in 'ocfs2_verify_group_and_inp ut()', corresponding buffer head		
			remains cached and subsequent call to the same 'ioctl()' for the same		
			inode issues the BUG() in 'ocfs2_set_new_buffer_upto date()' (trying		
			to cache the same buffer head of that inode). Fix this by uncaching		
			the buffer head with 'ocfs2_remove_from_cache()' on error path in		
			'ocfs2_group_add()'.		
			CVE ID : CVE-2024-53112		
Affected Vers	sion(s): From (i	ncluding)	4.20 Up to (excluding) 6.6.64		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/1 579483	
N/A	06-Dec-2024		netfilter: ipset: add missing range check in bitmap_ip_uadt	5378ed5 6fb9bac c6a5dd3 b9f3352	
		7.8	When tb[IPSET_ATTR_IP_TO] is not present but tb[IPSET_ATTR_CIDR] exists, the values of ip and ip_to are slightly swapped. Therefore, the range check	0604e, https:// git.kerne l.org/sta ble/c/3 5f56c55 4eb1b56 b77b3cf 197a6b0 0922d4 9033d,	
CVSSv3 Scoring	Scale 0-1	1-2 2	<mark>-3 3-4 4-5 5-6 </mark>	9033d, 6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for ip should be done later, but this part is missing and it seems that the vulnerability occurs. So we should add missing range checks and remove unnecessary range checks. CVE ID : CVE-2024-53141	https:// git.kerne l.org/sta ble/c/3c 20b594 8f119ae 61ee35a d8584d 666020c 91581	
Out-of- bounds Write	06-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: initramfs: avoid filename buffer overrun The initramfs filename field is defined in Documentation/driver- api/early-userspace/buffer- format.rst as: 37 cpio_file := ALGN(4) + cpio_header + filename + "\0" + ALGN(4) + data 55 ====== ===== 56 Field name Field size Meaning 57 ====== ==== 	https:// git.kerne l.org/sta ble/c/1a 423bbbe af9e3e2 0c46865 01efd9b 661fe83 4db, https:// git.kerne l.org/sta ble/c/4 9d01e73 6c30453 19e030d 1e75fb9 83011ab aca7, https:// git.kerne l.org/sta ble/c/bb 7ac9667 0ab1d8d 681015f 9d66e45 dad579a f4d	O-LIN-LINU- 241224/1503

4-5

5-6

6-7

7-8

8-9

9-10

3-4

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			70 c_namesize 8 bytes Length of filename, including final \0		
			When extracting an initramfs cpio archive, the kernel's do_name() path		
			handler assumes a zero- terminated path at @collected, passing it		
			directly to filp_open() / init_mkdir() / init_mknod().		
			If a specially crafted cpio entry carries a non-zero- terminated filename		
			and is followed by uninitialized memory, then a file may be created with		
			trailing characters that represent the uninitialized memory. The ability		
			to create an initramfs entry would imply already having full control of		
			the system, so the buffer overrun shouldn't be considered a security		
			vulnerability.		
			Append the output of the following bash script to an existing initramfs		
			and observe any created /initramfs_test_fname_over runAA* path. E.g.		
			./reproducer.sh gzip >> /myinitramfs		

0-1

1-2

Page **613** of **1137**

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It's easiest to observe non- zero uninitialized memory when the output is		
			gzipped, as it'll overflow the heap allocated @out_buf in gunzip(),		
			rather than the initrd_start+initrd_size block.		
			reproducer.sh nilchar="A" # change to "\0" to properly zero terminate / pad		
			magic="070701"		
			ino=1		
			mode=\$((0100777))		
			uid=0		
			gid=0		
			nlink=1		
			mtime=1		
			filesize=0		
			devmajor=0		
			devminor=1		
			rdevmajor=0		
			rdevminor=0		
			csum=0		
			fname="initramfs_test_fnam e_overrun"		
			namelen=\$((\${#fname} + 1)) # plus one to account for terminator		
			printf "%s%08x%08x%08x%08x		

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
			%08x%08x%08x%08x%08 x%08x%08x%08x%08x%s		
			"\		
			\$magic \$ino \$mode		
			\$uid \$gid \$nlink \$mtime \$filesize \		
			\$devmajor		
			\$devminor \$rdevmajor		
			\$rdevminor \$namelen \$csum \$fname		
			termpadlen=\$((1 + ((4 -		
			((110 + \$namelen) & 3)) % 4)))		
			printf "%.s\${nilchar}" \$(seq 1 \$termpadlen)		
			reproducer.sh		
			Symlink filename fields handled in do_symlink()		
			won't overrun past the		
			data segment, due to the		
			explicit zero-termination of the symlink		
			target.		
			Fix filename buffer overrun by aborting the initramfs		
			FSM if any cpio		
			entry doesn't carry a zero-		
			terminator at the expected (name_len - 1)		
			offset.		
			CVE ID : CVE-2024-53142		
Affected Vers	sion(s): From (i	ncluding)	4.4 Up to (excluding) 6.11.10	1	
Concurrent	02 D 2024	4 7	In the Linux kernel, the	https://	O-LIN-LINU-
Execution using	02-Dec-2024	4.7	following vulnerability has been resolved:	git.kerne l.org/sta	241224/1504
CVSSv3 Scoring *stands for all v		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
Shared Resource with Improper Synchroniz			net: fix data-races around sk->sk_forward_alloc	ble/c/0 73d898 08c065a c4c672c 0a613a7	
ation ('Race Condition')			Syzkaller reported this warning: [cut here] WARNING: CPU: 0 PID: 16	1b27a80 691cb, https:// git.kerne l.org/sta	
			at net/ipv4/af_inet.c:156 inet_sock_destruct+0x1c5/0 x1e0 44f2836	ble/c/d 285eb9d 0641c83	
			CPU: 0 UID: 0 PID: 16 Comm: ksoftirqd/0 Not tainted 6.12.0-rc5 #26	b7b3c5c c1b6	
			Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014		
			RIP: 0010:inet_sock_destruct+0x 1c5/0x1e0		
			Code: 24 12 4c 89 e2 5b 48 c7 c7 98 ec bb 82 41 5c e9 d1 18 17 ff 4c 89 e6 5b 48 c7 c7 d0 ec bb 82 41 5c e9 bf 18 17 ff 0f 0b eb 83 <0f> 0b eb 97 0f 0b eb 87 0f 0b e9 68 ff ff ff 66 66 2e 0f 1f 84 00		
			RSP: 0018:ffffc9000008bd90 EFLAGS: 00010206		
			RAX: 0000000000000300 RBX: ffff88810b172a90 RCX: 0000000000000007		

0-1

1-2

5-6

6-7

4-5

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RDX: 0000000000000002 RSI: 000000000000300 RDI: ffff88810b172a00		
			RBP: ffff88810b172a00 R08: ffff888104273c00 R09: 0000000000100007		
			R10: 0000000000020000 R11: 0000000000000006 R12: ffff88810b172a00		
			R13: 00000000000000004 R14: 0000000000000000 R15: ffff888237c31f78		
			FS: 000000000000000000000000000000000000		
			CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033		
			CR2: 00007ffc63fecac8 CR3: 00000000342e000 CR4: 00000000000006f0		
			DR0: 00000000000000000 DR1: 0000000000000000 DR2: 000000000000000000		
			DR3: 00000000000000000 DR6: 00000000fffe0ff0 DR7: 00000000000000400		
			Call Trace:		
			<task> ?_warn+0x88/0x130</task>		
			?		
			inet_sock_destruct+0x1c5/0 x1e0		
			?		
			report_bug+0x18e/0x1a0		
			? handle_bug+0x53/0x90 ?		
			? exc_invalid_op+0x18/0x70		
CVSSv3 Scoring		1-2 2	<mark>-3</mark> 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
			? asm_exc_invalid_op+0x1a/0 x20		
			? inet_sock_destruct+0x1c5/0 x1e0		
			_sk_destruct+0x2a/0x200		
			rcu_do_batch+0x1aa/0x530 ?		
			rcu_do_batch+0x13b/0x530		
			rcu_core+0x159/0x2f0		
			handle_softirqs+0xd3/0x2b 0		
			? pfx_smpboot_thread_fn+0 x10/0x10		
			run_ksoftirqd+0x25/0x30		
			smpboot_thread_fn+0xdd/0 x1d0		
			kthread+0xd3/0x100		
			?		
			pfx_kthread+0x10/0x10 ret_from_fork+0x34/0x50		
			?		
			pfx_kthread+0x10/0x10		
			ret_from_fork_asm+0x1a/0 x30		
			[end trace 0000000000000000]		
			Its possible that two threads call		

0-1

1-2

2-3

Demo (10 of 1127

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tcp_v6_do_rcv()/sk_forward _alloc_add()		
			concurrently when sk- >sk_state == TCP_LISTEN with sk->sk_lock unlocked,		
			which triggers a data-race around sk- >sk_forward_alloc:		
			tcp_v6_rcv		
			tcp_v6_do_rcv		
			skb_clone_and_charge_r		
			sk_rmem_schedule		
			sk_mem_schedule		
			sk_forward_alloc_add()		
			skb_set_owner_r		
			sk_mem_charge		
			sk_forward_alloc_add() kfree_skb skb_release_all		
			skb_release_head_state sock_rfree		
			sk_mem_uncharge		
			sk_forward_alloc_add()		
			sk_mem_reclaim		
			// set local var reclaimable		
			sk_mem_reclaim		
			sk_forward_alloc_add()		

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			In this syzkaller testcase, two threads call		
			tcp_v6_do_rcv() with skb- >truesize=768, the sk_forward_alloc changes like		
			this:		
			(cpu 1) (cpu 2) sk_forward_alloc		
			0		
			sk_mem_schedule() +4096 = 4096		
			 sk_mem_schedule() +4096 = 8192		
			sk_mem_charge() -768 = 7424		
			 sk_mem_charge() -768 = 6656		
			sk_mem_uncharge() +768 = 7424		
			reclaimable=7424 		
			 sk_mem_uncharge() +768 = 8192		
			 reclaimable=8192		
			sk_mem_reclaim() -4096 = 4096		
			 sk_mem_reclaim() -8192 = -4096 != 0		

 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
			The skb_clone_and_charge_r() should not be called in tcp_v6_do_rcv() when		
			sk->sk_state is TCP_LISTEN, it happens later in tcp_v6_syn_recv_sock().		
			Fix the same issue in dccp_v6_do_rcv().		
			CVE ID : CVE-2024-53124		
Affected Ver	sion(s): From (i	ncluding)	4.4.38 Up to (excluding) 4.5	1	
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/1	
			netlink: terminate outstanding dump on socket close	14a61d8 d94ae3a 43b824 46cf737f d75702	
			Netlink supports iterative dumping of data. It provides the families	1b834, https:// git.kerne l.org/sta	
			the following ops:	ble/c/1 76c41b3	O-LIN-LINU-
N/A	04-Dec-2024	5.5	- start - (optional) kicks off the dumping process	ca9281a 9736b6	241224/1505
			- dump - actual dump helper, keeps getting called until it returns 0	7c6121b 03dbf0c 8c08f,	
			- done - (optional) pairs with .start, can be used for cleanup	https:// git.kerne l.org/sta	
			The whole process is asynchronous and the repeated calls to .dump	ble/c/1 904fb9e bf91144 1f90a68	
			don't actually happen in a tight loop, but rather are triggered	e96b22a a73e441 0505	

0-1

1-2

2-3

3-4 4-5

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in response to recvmsg() on the socket.		
			This gives the user full control over the dump, but also means that		
			the user can close the socket without getting to the end of the dump.		
			To make sure .start is always paired with .done we check if there		
			is an ongoing dump before freeing the socket, and if so call .done.		
			The complication is that sockets can get freed from BH and .done		
			is allowed to sleep. So we use a workqueue to defer the call, when		
			needed.		
			Unfortunately this does not work correctly. What we defer is not		
			the cleanup but rather releasing a reference on the socket.		
			We have no guarantee that we own the last reference, if someone		
			else holds the socket they may release it in BH and we're back		
			to square one.		

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The whole dance, however, appears to be unnecessary. Only the user		
			can interact with dumps, so we can clean up when socket is closed.		
			And close always happens in process context. Some async code may		
			still access the socket after close, queue notification skbs to it etc.		
			but no dumps can start, end or otherwise make progress.		
			Delete the workqueue and flush the dump state directly from the release		
			handler. Note that further cleanup is possible in -next, for instance		
			we now always call .done before releasing the main module reference,		
			so dump doesn't have to take a reference of its own.		
Affected Ver	sion(s): From (i	ncluding)	CVE ID : CVE-2024-53140 4.8.14 Up to (excluding) 4.9		
		3	In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/1	
N/A	04-Dec-2024	5.5	netlink: terminate outstanding dump on socket close	14a61d8 d94ae3a 43b824 46cf737f d75702 1b834, https://	O-LIN-LINU- 241224/1506
CVSSv3 Scoring		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
			Netlink supports iterative dumping of data. It provides the families	git.kerne l.org/sta ble/c/1	
			the following ops:	76c41b3 ca9281a	
			- start - (optional) kicks off the dumping process	9736b6 7c6121b	
			- dump - actual dump helper, keeps getting called until it returns 0	03dbf0c 8c08f, https://	
			- done - (optional) pairs with .start, can be used for cleanup	git.kerne l.org/sta ble/c/1 904fb9e	
			The whole process is asynchronous and the repeated calls to .dump	bf91144 1f90a68 e96b22a	
			don't actually happen in a tight loop, but rather are triggered	a73e441 0505	
			in response to recvmsg() on the socket.		
			This gives the user full control over the dump, but also means that		
			the user can close the socket without getting to the end of the dump.		
			To make sure .start is always paired with .done we check if there		
			is an ongoing dump before freeing the socket, and if so call .done.		
			The complication is that sockets can get freed from BH and .done		

5-6 6-7 7-8

8-9

9-10

Page 624 of 1137

3-4

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is allowed to sleep. So we use a workqueue to defer the call, when		
			needed.		
			Unfortunately this does not work correctly. What we defer is not		
			the cleanup but rather releasing a reference on the socket.		
			We have no guarantee that we own the last reference, if someone		
			else holds the socket they may release it in BH and we're back		
			to square one.		
			The whole dance, however, appears to be unnecessary. Only the user		
			can interact with dumps, so we can clean up when socket is closed.		
			And close always happens in process context. Some async code may		
			still access the socket after close, queue notification skbs to it etc.		
			but no dumps can start, end or otherwise make progress.		
			Delete the workqueue and flush the dump state directly from the release		

0-1

1-2

2-3

Page **625** of **1137**

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handler. Note that further cleanup is possible in -next, for instance		
			we now always call .done before releasing the main module reference,		
			so dump doesn't have to take a reference of its own.		
			CVE ID : CVE-2024-53140		
Affected Ver	sion(s): From (i	ncluding)	4.9 Up to (excluding) 6.1.119		
		1 	In the Linux kernel, the following vulnerability has been resolved: netlink: terminate	https:// git.kerne l.org/sta ble/c/1 14a61d8	
			outstanding dump on socket close Netlink supports iterative dumping of data. It provides the families	d94ae3a 43b824 46cf737f d75702 1b834, https://	O-LIN-LINU- 241224/1507
			the following ops: - start - (optional) kicks off	git.kerne l.org/sta ble/c/1	
N/A	04-Dec-2024	5.5	the dumping process - dump - actual dump helper, keeps getting called until it returns 0	76c41b3 ca9281a 9736b6 7c6121b 03dbf0c 8c08f, https:// git.kerne	
			- done - (optional) pairs with .start, can be used for cleanup		
			The whole process is asynchronous and the repeated calls to .dump	l.org/sta ble/c/1 904fb9e	
			don't actually happen in a tight loop, but rather are triggered	bf91144 1f90a68 e96b22a a73e441	
			in response to recvmsg() on the socket.	0505	

4-5 3-4 2-3

5-6

7-8

8-9

9-10

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This gives the user full control over the dump, but also means that		
			the user can close the socket without getting to the end of the dump.		
			To make sure .start is always paired with .done we check if there		
			is an ongoing dump before freeing the socket, and if so call .done.		
			The complication is that sockets can get freed from BH and .done		
			is allowed to sleep. So we use a workqueue to defer the call, when		
			needed.		
			Unfortunately this does not work correctly. What we defer is not		
			the cleanup but rather releasing a reference on the socket.		
			We have no guarantee that we own the last reference, if someone		
			else holds the socket they may release it in BH and we're back		
			to square one.		

0-1

1-2

2-3

6-7

7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The whole dance, however, appears to be unnecessary. Only the user		
			can interact with dumps, so we can clean up when socket is closed.		
			And close always happens in process context. Some async code may		
			still access the socket after close, queue notification skbs to it etc.		
			but no dumps can start, end or otherwise make progress.		
			Delete the workqueue and flush the dump state directly from the release		
			handler. Note that further cleanup is possible in -next, for instance		
			we now always call .done before releasing the main module reference,		
			so dump doesn't have to take a reference of its own. CVE ID : CVE-2024-53140		
Affected Ver	sion(s): From (i	ncluding)	5.0 Up to (excluding) 6.1.119		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/aa	
N/A	04-Dec-2024	6.5	KVM: VMX: Bury Intel PT virtualization (guest/host mode) behind CONFIG_BROKEN	0d42cac f093a6fc ca872ed c954f6f8 12926a1 7, https://	O-LIN-LINU- 241224/1508
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
			Hide KVM's pt_mode module param behind CONFIG_BROKEN, i.e. disable support	git.kerne l.org/sta ble/c/b 91bb0ce	
			for virtualizing Intel PT via guest/host mode unless BROKEN=y. There are myriad bugs in the	5cd7005 b376eac 690ec66 4c1b563 72ec,	
			implementation, some of which are fatal to the guest,	https:// git.kerne	
			and others which put the stability and health of the host at risk.	l.org/sta ble/c/d 28b059e e4779b5	
			For guest fatalities, the most glaring issue is that KVM fails to ensure	102c5da 6e92976 252051 0e406	
			tracing is disabled, and *stays* disabled prior to VM-Enter, which is		
			necessary as hardware disallows loading (the guest's) RTIT_CTL if tracing		
			is enabled (enforced via a VMX consistency check). Per the SDM:		
			If the logical processor is operating with Intel PT enabled (if		
			IA32_RTIT_CTL.TraceEn = 1) at the time of VM entry, the "load		
			IA32_RTIT_CTL" VM-entry control must be 0.		
			On the host side, KVM doesn't validate the guest CPUID configuration		
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
			provided by userspace, and even worse, uses the guest configuration to		
			decide what MSRs to save/load at VM-Enter and VM-Exit. E.g. configuring		
			guest CPUID to enumerate more address ranges than are supported in hardware		
			will result in KVM trying to passthrough, save, and load non-existent MSRs,		
			which generates a variety of WARNs, ToPA ERRORs in the host, a potential		
			deadlock, etc.		
			CVE ID : CVE-2024-53135		
Affected Ver	sion(s): From (i	ncluding)	5.1 Up to (excluding) 6.1.119	•	
	02-Dec-2024		In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/0	
Concurrent Execution			net/mlx5: fs, lock FTE when checking if active	94d1a21 21cee1e 85ab07d 74388f9	
using Shared Resource with		5.5	The referenced commits introduced a two-step process for deleting FTEs:	4809dcf b5b9, https://	O-LIN-LINU-
with Improper Synchroniz ation ('Race Condition')		5.5	- Lock the FTE, delete it from hardware, set the hardware deletion function	git.kerne l.org/sta ble/c/9 33ef0d1 7f012b6	241224/1509
			to NULL and unlock the FTE.	53e9e60 06e3f50 c8d0238	
			- Lock the parent flow group, delete the software copy of the FTE, and	b5ed, https:// git.kerne	
			remove it from the xarray.	l.org/sta	
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
			However, this approach encounters a race condition if a rule with the same match value is added simultaneously. In this scenario, fs_core may set the	ble/c/9c a314419 930f913 5727e39 d77e662 62d5f7b ef6	
			hardware deletion function to NULL prematurely, causing a panic during		
			subsequent rule deletions.		
			To prevent this, ensure the active flag of the FTE is checked under a lock, which will prevent the fs_core layer from attaching a new steering rule to		
			an FTE that is in the process		
			of deletion.		
			[438.967589] MOSHE: 2496 mlx5_del_flow_rules del_hw_func		
			[438.968205][cut here]		
			[438.968654] refcount_t: decrement hit 0; leaking memory.		
			[438.969249] WARNING: CPU: 0 PID: 8957 at lib/refcount.c:31 refcount_warn_saturate+0xf		
			b/0x110 [438.970054] Modules linked in: act_mirred cls_flower act_gact sch_ingress openvswitch		

Page **631** of **1137**

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
weakiless		00305	nsh mlx5_vdpa vringh vhost_iotlb vdpa mlx5_ib mlx5_core xt_conntrack xt_MASQUERADE nf_conntrack_netlink nfnetlink xt_addrtype iptable_nat nf_nat br_netfilter rpcsec_gss_krb5 auth_rpcgss oid_registry overlay rpcrdma rdma_ucm ib_iser libiscsi scsi_transport_iscsi ib_umad rdma_cm ib_ipoib iw_cm ib_cm ib_uverbs ib_core zram zsmalloc fuse [last unloaded: cls_flower]	Fatch	
			[438.973288] CPU: 0 UID: 0 PID: 8957 Comm: tc Not tainted 6.12.0-rc1+ #8 [438.973888] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0- gf21b5a4aeb02- prebuilt.qemu.org 04/01/2014		
			[438.974874] RIP: 0010:refcount_warn_satura te+0xfb/0x110		
			[438.975363] Code: 40 66 3b 82 c6 05 16 e9 4d 01 01 e8 1f 7c a0 ff 0f 0b c3 cc cc cc cc 48 c7 c7 10 66 3b 82 c6 05 fd e8 4d 01 01 e8 05 7c a0 ff <0f> 0b c3 cc cc cc cc 66 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 90		
			[438.976947] RSP: 0018:ffff888124a53610 EFLAGS: 00010286		
			[438.977446] RAX: 0000000000000000 RBX:		
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
			ffff888119d56de0 RCX: 0000000000000000		
			[438.978090] RDX: ffff88852c828700 RSI: ffff88852c81b3c0 RDI: ffff88852c81b3c0		
			[438.978721] RBP: ffff888120fa0e88 R08: 0000000000000000 R09: ffff888124a534b0		
			[438.979353] R10: 0000000000000001 R11: 0000000000000001 R12: ffff888119d56de0		
			[438.979979] R13: ffff888120fa0ec0 R14: ffff888120fa0ee8 R15: ffff888119d56de0		
			[438.980607] FS: 00007fe6dcc0f800(0000) GS:ffff88852c800000(0000) knlGS:00000000000000000		
			[438.983984] CS: 0010 DS: 0000 ES: 0000 CR0: 000000080050033		
			[438.984544] CR2: 00000000004275e0 CR3: 0000000186982001 CR4: 000000000372eb0		
			[438.985205] DR0: 0000000000000000 DR1: 000000000000000 DR2: 00000000000000000		
			[438.985842] DR3: 0000000000000000 DR6: 000000000fffe0ff0 DR7: 00000000000000400		
			[438.986507] Call Trace:		
			[438.986799] <task></task>		

3-4 4-5 5-6 6-7

7-8 8-9

9-10

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<pre>[438.987070] ?warn+0x7d/0x110 [438.987426] ? refcount_warn_saturate+0xf b/0x110</pre>		
			[438.987877] ? report_bug+0x17d/0x190		
			[438.988261] ? prb_read_valid+0x17/0x20		
			[438.988659] ? handle_bug+0x53/0x90		
			[438.989054] ? exc_invalid_op+0x14/0x70		
			[438.989458] ? asm_exc_invalid_op+0x16/0 x20		
			[438.989883] ? refcount_warn_saturate+0xf b/0x110		
			[438.990348] mlx5_del_flow_rules+0x2f7/ 0x340 [mlx5_core]		
			[438.990932] mlx5_eswitch_del_rule+0x 49/0x170 [mlx5_core]		
			[438.991519] ? mlx5_lag_is_sriov+0x3c/0x5 0 [mlx5_core]		
			[438.992054] ? xas_load+0x9/0xb0		
			[438.992407] mlx5e_tc_rule_unoffload+0x 45/0xe0 [mlx5_core]		
			[438.993037] mlx5e_tc_del_fdb_flow+0x2 a6/0x2e0 [mlx5_core]		
			[438.993623] mlx5e_flow_put+0x29/0x60 [mlx5_core]		
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
			[438.994161] mlx5e_delete_flower+0x261 /0x390 [mlx5_core]		
			[438.994728] tc_setup_cb_destroy+0xb9/ 0x190		
			[438.995150] fl_hw_destroy_filter+0x94/ 0xc0 [cls_flower]		
			[438.995650] fl_change+0x11a4/0x13c0 [cls_flower]		
			[438.996105] tc_new_tfilter+0x347/0xbc0		
			[438.996503] ?		
			truncated		
			CVE ID : CVE-2024-53121		
Affected Ver	sion(s): From (i	ncluding)	5.10 Up to (excluding) 6.1.119	1	Г
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/2	
		2-Dec-2024 5.5	virtio/vsock: Fix accept_queue memory leak	415345 042245 de7601d cc6eafdb	
Missing Release of Memory after Effective Lifetime	02-Dec-2024		As the final stages of socket destruction may be delayed, it is possible	e3a3dcc 9e379, https:// git.kerne	O-LIN-LINU- 241224/1510
			that virtio_transport_recv_listen () will be called after the accept_queue	l.org/sta ble/c/8 97617a4 13e0bf1	
			has been flushed, but before the SOCK_DONE flag has been set. As a result,	c6380e3 b34b2f2 8f45050 8549,	
			sockets enqueued after the flush would remain unremoved, leading to a	https:// git.kerne l.org/sta	
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
			memory leak.	ble/c/9	
				46c7600 fa2207c	
			vsock_release	c8d3fbc	
			vsock_release	86a518e	
			lock	c56f98a 5813	
			virtio_transport_release	5015	
			virtio_transport_close		
			schedule_delayed_work(clo se_work)		
			sk_shutdown =		
			SHUTDOWN_MASK		
			(!) flush accept_queue		
			release		
			virtio_transport_recv_pkt		
			vsock_find_bound_socket		
			lock		
			if		
			flag(SOCK_DONE) return		
			virtio_transport_recv_listen		
			child = vsock_create_connected		
			(!)		
			vsock_enqueue_accept(child		
)		
			release		
			close_work		
			lock		
			virtio_transport_do_close		
			set_flag(SOCK_DONE)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			virtio_transport_remove_so ck		
			vsock_remove_sock		
			vsock_remove_bound		
			release		
			Introduce a sk_shutdown check to disallow vsock_enqueue_accept() during socket destruction.		
			unreferenced object 0xffff888109e3f800 (size 2040):		
			comm "kworker/5:2", pid 371, jiffies 4294940105		
			hex dump (first 32 bytes):		
			00 00 00 00 00 00 00 00 00 00 00 00 00 0		
			28 00 0b 40 00 00 00 00 00 00 00 00 00 00 00 00 00		
			backtrace (crc 9e5f4e84):		
			[<ffffffff81418ff1>] kmem_cache_alloc_noprof+ 0x2c1/0x360</ffffffff81418ff1>		
			[<ffffffff81d27aa0>] sk_prot_alloc+0x30/0x120</ffffffff81d27aa0>		
			[<ffffffff81d2b54c>] sk_alloc+0x2c/0x4b0</ffffffff81d2b54c>		
			 [<fffffff81fe049a>]</fffffff81fe049a>		
			vsock_create.constprop.0+ 0x2a/0x310		

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[<fffffff81fe6d6c>] virtio_transport_recv_pkt+0 x4dc/0x9a0</fffffff81fe6d6c>		
			[<ffffffff81fe745d>] vsock_loopback_work+0xfd /0x140</ffffffff81fe745d>		
			[<ffffffff810fc6ac>] process_one_work+0x20c/0 x570</ffffffff810fc6ac>		
			[<ffffffff810fce3f>] worker_thread+0x1bf/0x3a 0</ffffffff810fce3f>		
			[<fffffffff811070dd>] kthread+0xdd/0x110</fffffffff811070dd>		
			[<ffffffff81044fdd>] ret_from_fork+0x2d/0x50</ffffffff81044fdd>		
			[<ffffffff8100785a>] ret_from_fork_asm+0x1a/0 x30</ffffffff8100785a>		
			CVE ID : CVE-2024-53119		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/2 499585	
Concurrent Execution using Shared			mptcp: cope racing subflow creation in mptcp_rcv_space_adjust	1d58c4a 205ad0f fa7b2f2 1e479a9	
Resource with 02-Dec-2 Improper Synchroniz ation ('Race Condition')	02-Dec-2024		Additional active subflows - i.e. created by the in kernel path	c8527, https:// git.kerne l.org/sta ble/c/aa	O-LIN-LINU- 241224/1511
			manager - are included into the subflow list before starting the	d6412c6 3baa39d d813e81	
			3whs.	f16a14d 976b3de 2e8,	
				https://	

0-1

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

A racing recvms() spooling data received on an already establishedgit.kerne l.org/sta ble/c/ce 7356ae3subflow would unconditionally call tcp_cleanup_rbuf() on all the current subflows, potentially hitting a divide by zero error on the newly created ones.5943cc6 2462d51 ar34062 b7dAffected Version(s): From (including) Shared Resource with Improper Synchroniz ationIn the Linux kernel, the following vulnerability has been resolved:https:// git.kerne bie/c/3 64537e8 a32a2Affected Version(s): From (including) Shared Resource with Improper Synchroniz ation04-Dec-2024Revert d949d1d14fa2 ("m:: shmem: fix data-race in in shmem_getattr()" as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over Spication"01.IN-LINU- 241224/1512Affected Version(a ation ("Race Condition")04-Dec-20244.7Revert d949d1d14fa2 ("m:: shmem: fix data-race in in shmem_getattr()" as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over Spication ("Race Condition")0-LIN-LINU- 241224/1512As Hugh commented, "added just to silence a "added just to silence a	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version (s): From (including)5.10.229 Up to (excluding) 5.11Affected Version (s): From (including)5.10.229 Up to (excluding) 5.11Kender (s): From (including)5.10.229 Up to (excluding) 5.11Kender (s): From (including)1.11Kender (s): From (s):				data received on an already established subflow would unconditionally call tcp_cleanup_rbuf() on all the current subflows, potentially hitting a divide by zero error on the newly created ones. Explicitly check that the subflow is in a suitable state before invoking tcp_cleanup_rbuf().	l.org/sta ble/c/ce 7356ae3 5943cc6 494cc69 2e62d51 a734062	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')04-Dec-2024 V4.7In the Linux kernel, the following vulnerability has been resolved:git.kerne Lorg/sta ble/c/3 6b537e8 d88a3a2 2d52, https://0-LIN-LINU- 241224/1512With Improper Synchroniz ation ('Race Condition')04-Dec-2024 With Improper Synchroniz ation ('Race Condition')4.7Revert d949d1d14fa2 ("mm: shmem: fix data-race in shmem_getattr()") as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over NFS.0-LIN-LINU- 241224/1512Kevert d949d1d14fa2 ("mm: shmem_fix data-race in shmem_getattr()") as ble/c/50-LIN-LINU- 241224/1512Kevert d949d1d14fa2 ("mm: shmem_fix data-race in shmem_getattr()") as ble/c/50-LIN-LINU- 241224/1512Kevert d949d1d14fa2 ("mm: shmem.fix data-race in shmem_getattr()") as 	Affected Ver	<mark>sion(s): From (i</mark>	ncluding)		1	
	Execution using Shared Resource with Improper Synchroniz ation ('Race	04-Dec-2024	4.7	following vulnerability has been resolved: mm: revert "mm: shmem: fix data-race in shmem_getattr()" Revert d949d1d14fa2 ("mm: shmem: fix data-race in shmem_getattr()") as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over NFS. As Hugh commented,	git.kerne l.org/sta ble/c/3 6b537e8 f302f67 0c7cf35 d88a3a2 94443e3 2d52, https:// git.kerne l.org/sta ble/c/5 874c115 0e77296 565ad6e 495ef41 fbf8757 0d14, https://	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): From (i	ncluding)	syzbot sanitizer splat: added where there has never been any practical problem". CVE ID : CVE-2024-53136 5.13 Up to (excluding) 6.1.119	l.org/sta ble/c/6 4e67e86 94252c1 bf01b80 2ee911b e3fee62 c36b	
NULL Pointer Dereferenc e	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm: fix NULL pointer dereference in alloc_pages_bulk_noprof We triggered a NULL pointer dereference for ac.preferred_zoneref->zone in alloc_pages_bulk_noprof() when the task is migrated between cpusets. When cpuset is enabled, in prepare_alloc_pages(), ac- >nodemask may be ¤t->mems_allowed. when first_zones_zonelist() is called to find preferred_zoneref, the ac- >nodemask may be modified concurrently if the task is migrated between different cpusets. Assuming we have 2 NUMA Node,	https:// git.kerne l.org/sta ble/c/3 150237 4627ba9 ec3e710 dbd0bb 00457cc 6d2c19, https:// git.kerne l.org/sta ble/c/6a ddb2d9 501ec86 6d7b3a3 b4e6653 07c437e 9be2, https:// git.kerne l.org/sta ble/c/8c e41b0f9 d77cca0 74df25a fd39b86 e2ee3aa 68e	O-LIN-LINU- 241224/1513

4-5 5-6 6-7

7-8

8-9

9-10

1-2

2-3

0-1

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			when traversing Node1 in ac->zonelist, the nodemask is 2, and when					
			traversing Node2 in ac- >zonelist, the nodemask is 1. As a result, the					
			ac->preferred_zoneref points to NULL zone.					
			In alloc_pages_bulk_noprof(), for_each_zone_zonelist_nod emask() finds a					
			allowable zone and calls zonelist_node_idx(ac.prefer red_zoneref), leading					
			to NULL pointer dereference.					
			alloc_pages_noprof() fixes this issue by checking NULL pointer in commit					
			ea57485af8f4 ("mm, page_alloc: fix check for NULL preferred_zone") and					
			commit df76cee6bbeb ("mm, page_alloc: remove redundant checks from alloc					
			fastpath").					
			To fix it, check NULL pointer for preferred_zoneref->zone.					
			CVE ID : CVE-2024-53113					
Affected Ver	Affected Version(s): From (including) 5.14 Up to (excluding) 6.1.119							

5-6 6-7 7-8 8-9

9-10

3-4

2-3

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness NULL Pointer Dereferenc e	Publish Date	CVSSv3	Description & CVE ID In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: CT: Fix null-ptr- deref in add rule err flow In error flow of mlx5_tc_ct_entry_add_rule() , in case ct_rule_add() callback returns error, zone_rule->attr is used uninitiated. Fix it to use attr which has the needed pointer value. Kernel log: BUG: kernel NULL pointer dereference, address: 00000000000110 RIP: 0010:mlx5_tc_ct_entry_add_ rule+0x2b1/0x2f0 [mlx5_core] Call Trace: <task> ?die+0x20/0x70 ? page_fault_oops+0x150/0x 3e0 ? exc_page_fault+0x74/0x140 ? asm_exc_page_fault+0x22/0 x30</task>	Patch https:// git.kerne l.org/sta ble/c/0 6dc488a 593020 bd2f006 798557 d2a3210 4d8359, https:// git.kerne l.org/sta ble/c/0c 7c70ff8b 696cfed ba35041 1dca736 361ef9a 0f, https:// git.kerne l.org/sta ble/c/6 030f8bd 7902e9e 276a0ed c09bf11 979e4e2 bc2e	NCIIPC ID

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? mlx5_tc_ct_entry_add_rule+ 0x2b1/0x2f0 [mlx5_core] ? mlx5_tc_ct_entry_add_rule+ 0x1d5/0x2f0 [mlx5_core]		
			mlx5_tc_ct_block_flow_offlo ad+0xc6a/0xf90 [mlx5_core] ? nf_flow_offload_tuple+0xd8 /0x190 [nf_flow_table]		
			nf_flow_offload_tuple+0xd8 /0x190 [nf_flow_table]		
			flow_offload_work_handler+ 0x142/0x320 [nf_flow_table] ? finish_task_switch.isra.0+0x 15b/0x2b0		
			process_one_work+0x16c/0 x320		
			worker_thread+0x28c/0x3a 0 ? pfx_worker_thread+0x10/ 0x10		
			kthread+0xb8/0xf0 ? pfx_kthread+0x10/0x10 ret_from_fork+0x2d/0x50 ?		
			? pfx_kthread+0x10/0x10		

0-1

1-2

3-4 4-5

5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Ver	sion(s): From (i	ncluding)	ret_from_fork_asm+0x1a/0 x30 CVE ID : CVE-2024-53120 5.15.171 Up to (excluding) 5.1				
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	04-Dec-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: mm: revert "mm: shmem: fix data-race in shmem_getattr()" Revert d949d1d14fa2 ("mm: shmem: fix data-race in shmem_getattr()") as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over NFS. As Hugh commented, "added just to silence a syzbot sanitizer splat: added where there has never been any practical problem". CVE ID : CVE-2024-53136	https:// git.kerne l.org/sta ble/c/3 6b537e8 f302f67 0c7cf35 d88a3a2 94443e3 2d52, https:// git.kerne l.org/sta ble/c/5 874c115 0e77296 565ad6e 495ef41 fbf8757 0d14, https:// git.kerne l.org/sta ble/c/6 4e67e86 94252c1 bf01b80 2ee911b e3fee62 c36b	O-LIN-LINU- 241224/1515		
Affected Ver	Affected Version(s): From (including) 5.19 Up to (excluding) 6.1.119						
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/0a 886489	O-LIN-LINU- 241224/1516		
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<pre>vp_vdpa: fix id_table array not null terminated error Allocate one extra virtio_device_id as null terminator, otherwise vdpa_mgmtdev_get_classes() may iterate multiple times and visit undefined memory. CVE ID : CVE-2024-53110</pre>	d27459 6ad1a80 789d3a7 735032 10a615, https:// git.kerne l.org/sta ble/c/4e 39ecadf 1d2a081 871396 19f1f31 4b64ba7 d947, https:// git.kerne l.org/sta ble/c/8 70d68fe 17b5d9 032049 dcad98b 5781a34 4a8657	
Affected Ver	sion(s): From (i	ncluding)	5.4 Up to (excluding) 6.1.119		
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: kTLS, Fix incorrect page refcounting The kTLS tx handling code is using a mix of get_page() and page_ref_inc() APIs to increment the page reference. But on the release	https:// git.kerne l.org/sta ble/c/2 723e8b2 cbd486c b96e5a6 1b2247 3f7fd62 e18df, https:// git.kerne l.org/sta ble/c/6 9fbd07f 17b0fda f8970bc	O-LIN-LINU- 241224/1517

0-1

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Descr	iption & C	VE ID		Patch	NCII	PC ID
			path (mlx5e_kt nc_dump_ put_page(comp()),	only	7 11 83 ht	05f5bf 15c297 39d, ttps:// t.kerne		
			This is an pages from get_page(references folio page	n large fo) s are stor	olios: the	⁸ bl ⁹ 3a b9 ne 48	org/sta e/c/9 a14620 97c911 89a5b0 8782f3		
			page_ref_i references directly in On release	nc() s are stor the give	ed n page.	d	9b0c4a ff4		
			page will too many		erenced				
			This was f kTLS testi + ZC wher	ng with s					
			served file NFS on a l large folio	kernel wi s suppor	th NFS t				
			(commit 4 ("nfs: add folios")).	support	for large				
Affected Vor	sion(s): From (including	CVE ID : (
Concurrent Execution using Shared Resource			In the Lin following been reso	ux kernel vulnerab	, the	ht gi l.c bl 6t	ttps:// t.kerne org/sta e/c/3 o537e8	O-LIN-L	INIL
with Improper Synchroniz ation ('Race Condition')	04-Dec-2024	4.7	mm: rever fix data-ra shmem_ge	ice in	hmem:	00 d8 94 20 ht	02f67 c7cf35 38a3a2 4443e3 d52, ttps:// t.kerne	0-LIN-L 241224	
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
			Revert d949d1d14fa2 ("mm: shmem: fix data-race in shmem_getattr()") as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over NFS. As Hugh commented, "added just to silence a syzbot sanitizer splat:	l.org/sta ble/c/5 874c115 0e77296 565ad6e 495ef41 fbf8757 0d14, https:// git.kerne l.org/sta ble/c/6	
Affected Ver	sion(s): From (i	ncluding)	added where there has never been any practical problem". CVE ID : CVE-2024-53136 6.1 Up to (excluding) 6.6.63	4e67e86 94252c1 bf01b80 2ee911b e3fee62 c36b	
Aniceted Ver			In the Linux kernel, the	https://	
			following vulnerability has been resolved: pmdomain: imx93-blk-ctrl: correct remove path	git.kerne l.org/sta ble/c/2 01fb9e1 64a1e4c 5937de2	
Always- Incorrect Control Flow Implement ation	04-Dec-2024	5.5	The check condition should be 'i < bc- >onecell_data.num_domains ', not 'bc- >onecell_data.num_domains ' which will make the look never finish and cause kernel panic.	cf58bcb 0327c08 664f, https:// git.kerne l.org/sta ble/c/8f c228ab5 d38a026 eae7183 a5f74a4f	O-LIN-LINU- 241224/1519
			Also disable runtime to address "imx93-blk-ctrl 4ac10000.system-	ac43d9b 6a, https:// git.kerne l.org/sta ble/c/f7	

0-1

1-2

2-3

Page 647 of 1137

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): From (i	ncluding)	controller: Unbalanced pm_runtime_enable!" CVE ID : CVE-2024-53134 6.1.0 Up to (excluding) 6.1.119	c7c5aa5 56378a2 c8da72c 1f7f238 b6648f9 5fb	
NULL Pointer Dereferenc e	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/rockchip: vop: Fix a dereferenced before check warning The 'state' can't be NULL, we should check crtc_state. Fix warning: drivers/gpu/drm/rockchip /rockchip_drm_vop.c:1096 vop_plane_atomic_async_ch eck() warn: variable dereferenced before check 'state' (see line 1077) CVE ID : CVE-2024-53129	https:// git.kerne l.org/sta ble/c/1e 530597 29691ca 4d9051 18258b 9fbd17d 854174, https:// git.kerne l.org/sta ble/c/6 56dbd1c 21c2c08 8c70059 cdd43ec 83e7d54 ec4d, https:// git.kerne l.org/sta ble/c/ab 1c793f4 57f740a b7108cc 0b1340a 402dbf4 84d	O-LIN-LINU- 241224/1520
Affected Vers	sion(s): From (i	ncluding)	6.1.110 Up to (excluding) 6.1.1	119	
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/0	O-LIN-LINU- 241224/1521
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
vveakness		CVSSV3	Description & CVE IDRevert "mmc: dw_mmc: Fix IDMAC operation with pages bigger than 4K"The commit 8396c793ffdf ("mmc: dw_mmc: Fix IDMAC operation with pagesbigger than 4K") increased the max_req_size, even for 4K pages, causing various issues: - Panic booting the kernel/rootfs from an SD card on Rockchip RK3566 - Panic booting the kernel/rootfs from an SD card on StarFive JH7100 - "swiotlb buffer is full" and data corruption on StarFive JH7110At this stage no fix have been found, so it's probably better to just revert the change.This reverts commit 8396c793ffdf28bb8aee7cfe 0891080f8cab7890.	Patch 0bff717 45bc358 3bd5ca5 9be91e0 ee1d27f 1944, https:// git.kerne l.org/sta ble/c/1 635e407 a4a64d0 8a8517a c59ca14 ad4fc78 5e75, https:// git.kerne l.org/sta ble/c/5 6de724c 58c07a7 ca3aac0 27cfd2c cb184ed 9e4e	
			CVE ID : CVE-2024-53127		
	sion(s): From (i	ncluding)	6.1.116 Up to (excluding) 6.1.1		
Concurrent Execution using Shared Resource with Improper	04-Dec-2024	4.7	In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/3 6b537e8 f302f67 0c7cf35	O-LIN-LINU- 241224/1522
CVSSv3 Scoring *stands for all v		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
Synchroniz ation ('Race Condition')			mm: revert "mm: shmem: fix data-race in shmem_getattr()"	d88a3a2 94443e3 2d52, https://	
			Revert d949d1d14fa2 ("mm: shmem: fix data-race in shmem_getattr()") as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over	git.kerne l.org/sta ble/c/5 874c115 0e77296 565ad6e 495ef41	
			NFS. As Hugh commented,	fbf8757 0d14, https:// git.kerne	
			"added just to silence a syzbot sanitizer splat: added where there has never been	l.org/sta ble/c/6 4e67e86 94252c1	
			any practical problem". CVE ID : CVE-2024-53136	bf01b80 2ee911b e3fee62 c36b	
Affected Ver	<mark>sion(s): From (</mark> i	ncluding)	6.1.60 Up to (excluding) 6.1.11	19	
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta	
Concurrent Execution using Shared			mptcp: error out earlier on disconnect	ble/c/5 813022 98524e9 d77c4c4 4ff5156	
Resource with Improper Synchroniz	02-Dec-2024	5.5	Eric reported a division by zero splat in the MPTCP protocol:	a6cd112 227ae, https:// git.kerne	O-LIN-LINU- 241224/1523
ation ('Race Condition')			Oops: divide error: 0000 [#1] PREEMPT SMP KASAN PTI CPU: 1 UID: 0 PID: 6094	l.org/sta ble/c/9 55388e1 d5d222c 4101c59	
CVSSv3 Scoring	Scale 0-1	1-2 2	Comm: syz-executor317 Not tainted	6b536d 41b91a8	8-9 9-10

Weakness	Publish Date	CVSSv3	Descrip	otion & C	VE ID	F	atch	NCIII	PC ID
			6.12.0-rc5- g05b92660 Hardware b Google Con Engine/Go Engine,	Ocdfe #0 name: G npute ogle Cor	oogle npute	htt git l.or ble 68	12e, ps:// .kerne rg/sta e/c/a6 05c9b caf4e		
			BIOS Googl RIP: 0010:tcp_ 0x5b4/0x1 net/ipv4/t Code: f6 44	_select_v .310 cp_outp	window+ ut.c:3163	16 83 01	af7a6 f6c6b c90d1 0		
			9b 75 09 f8 11 ff ff ff e8 0d 74 09 f8 ff ff e8 00 7 99 <f7> 7c</f7>	8 44 39 f 8 8 45 89 f	3 0f 8d 4 e9 04 f	f			
			24 14 41 29 ec fe ff ff e8 89 RSP: 0018:ffffc9	3 e8 73 0	9 f8 48				
			EFLAGS: 00 RAX: 00000 RBX: 00000 RCX: ffffffff	0010293 0000000 0000000 898331	3 017e67 017e67 4b				
			RDX: 0000 RSI: ffffffff 000000000 RBP: 00000 R08: 00000	398331b 0000000 0000005	00 RDI: 04 5d6000				
			R09: 00000 R10: 00000 R11: 00000 R12: 00000)000000()000000()000000()03e80)00000)03e80				
			R13: ffff888 R14: 00000 R15: 00000 FS: 00007feb5	0000000 0000002	017e67 2eb000				
CVSSv3 Scoring	Scale 0-1	1-2 2	<mark>-3</mark> 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GS:ffff8880b8700000(0000		
) knlGS:0000000000000000000		
			CS: 0010 DS: 0000 ES: 0000		
			CR0: 0000000080050033		
			CR2: 00007feb5d8adbb8		
			CR3: 0000000074e4c000 CR4: 0000000003526f0		
			DR0: 00000000000000000		
			DR1: 00000000000000000 DR2: 00000000000000000		
			DR3: 00000000000000000		
			DR6: 00000000fffe0ff0 DR7: 0000000000000400		
			Call Trace:		
			<task></task>		
			tcp_cleanup_rbuf+0x3e7/ 0x4b0 net/ipv4/tcp.c:1493		
			mptcp_rcv_space_adjust net/mptcp/protocol.c:2085		
			[inline]		
			mptcp_recvmsg+0x2156/0x 2600		
			net/mptcp/protocol.c:2289		
			inet_recvmsg+0x469/0x6a0 net/ipv4/af_inet.c:885		
			sock_recvmsg_nosec net/socket.c:1051 [inline]		
			sock_recvmsg+0x1b2/0x25 0 net/socket.c:1073		
			sys_recvfrom+0x1a5/0x2 e0 net/socket.c:2265		
			do_sys_recvfrom net/socket.c:2283 [inline]		
			se_sys_recvfrom		
			net/socket.c:2279 [inline]		
			x64_sys_recvfrom+0xe0/0 x1c0 net/socket.c:2279		

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_syscall_x64 arch/x86/entry/common.c: 52 [inline]		
			do_syscall_64+0xcd/0x250 arch/x86/entry/common.c: 83		
			entry_SYSCALL_64_after_hw frame+0x77/0x7f		
			RIP: 0033:0x7feb5d857559		
			Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 51 18 00 00 90 48 89 f8 48		
			89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d		
			01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48		
			RSP: 002b:00007feb5d7f1208 EFLAGS: 00000246 ORIG_RAX: 00000000000002d		
			RAX: fffffffffffffffda RBX: 00007feb5d8e1318 RCX: 00007feb5d857559		
			RDX: 000000800000000 RSI: 0000000000000000 RDI: 00000000000000003		
			RBP: 00007feb5d8e1310 R08: 00000000000000000 R09: fffffff81000000		
			R10: 00000000000000100 R11: 000000000000246 R12: 00007feb5d8e131c		
			R13: 00007feb5d8ae074 R14: 000000800000000e R15: 00000000fffffdef		

4-5 5-6 6-7

7-8 8-9 9-10

0-1

1-2

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and provided a nice reproducer.		
			The root cause is the current bad handling of racing disconnect.		
			After the blamed commit below, sk_wait_data() can return (with		
			error) with the underlying socket disconnected and a zero rcv_mss.		
			Catch the error and return without performing any additional		
			operations on the current socket.		
			CVE ID : CVE-2024-53123		
Affected Ver	sion(s): From (i	ncluding)	6.10 Up to (excluding) 6.11.10		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/3	
			drm/panthor: Fix handling of partial GPU mapping of BOs	387e043 918e154 ca08d83 954966a 8b087fe	
N/A	02-Dec-2024	5.5	This commit fixes the bug in the handling of partial mapping of the	2835, https:// git.kerne	O-LIN-LINU- 241224/1524
			buffer objects to the GPU, which caused kernel warnings.	l.org/sta ble/c/d 3e61af6 4b770e0 038470c	
			Panthor didn't correctly handle the case where the partial mapping	81f42bd 1d0598f 6bcc	
CVSSv3 Scoring		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
			spanned multiple scatterlists and the mapping offset didn't point		
			to the 1st page of starting scatterlist. The offset variable was		
			not cleared after reaching the starting scatterlist.		
			Following warning messages were seen.		
			WARNING: CPU: 1 PID: 650 at drivers/iommu/io- pgtable-arm.c:659 arm_lpae_unmap+0x254/ 0x5a0		
			<snip></snip>		
			pc : arm_lpae_unmap+0x254/ 0x5a0		
			lr : arm_lpae_unmap+0x2cc/0 x5a0		
			<snip></snip>		
			Call trace:		
			arm_lpae_unmap+0x254/ 0x5a0		
			arm_lpae_unmap+0x108/ 0x5a0		
			arm_lpae_unmap+0x108/ 0x5a0		
			arm_lpae_unmap+0x108/ 0x5a0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arm_lpae_unmap_pages+0x 80/0xa0		
			panthor_vm_unmap_pages+ 0xac/0x1c8 [panthor]		
			panthor_gpuva_sm_step_un map+0x4c/0xc8 [panthor]		
			op_unmap_cb.isra.23.constp rop.30+0x54/0x80		
			drm_gpuvm_sm_unmap+0 x184/0x1c8		
			drm_gpuvm_sm_unmap+0x 40/0x60		
			panthor_vm_exec_op+0xa8/ 0x120 [panthor]		
			panthor_vm_bind_exec_sync _op+0xc4/0xe8 [panthor]		
			panthor_ioctl_vm_bind+0x1 0c/0x170 [panthor]		
			drm_ioctl_kernel+0xbc/0x1 38		
			drm_ioctl+0x210/0x4b0		
			arm64_sys_ioctl+0xb0/0xf 8		
			invoke_syscall+0x4c/0x110		
			el0_svc_common.constprop. 1+0x98/0xf8		
			do_el0_svc+0x24/0x38		
CVSSv3 Scoring		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10
*stands for all v	versions		Page 656 of 1127		

Weakness	Publish Date	CVSSv3		Descri	ption & C	VE ID		Pat	ch	NCII	PC ID
			el)_svc+02	x34/0xc	8					
			el0	t 64 sy	nc hand	ler+0xa(0				
				xc8	_						
			el)t_64_sy	mc+0x1	74/0x17	'8				
				nip>							
			drr			imappec int)	d_				
			at dri pai pai	vers/gp nthor_m nthor_vr	ou/drm/ mu.c:92	p_pages	/				
			<sr< td=""><td>nip></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></sr<>	nip>							
			-	nthor_vr	n_unma lc8 [pan	p_pages [.] thor]	+				
			-		n_unma lc8 [pan	p_pages [.] thor]	+				
			<sr< td=""><td>nip></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></sr<>	nip>							
			fail ffff	ed to ur a388f00	drm] *E 1map rai 00-ffffa3	nge					
			-	quested a388c0(-	890000	٦				
						I-53116	-				
			fol			, the ility has	۹ ۱ ۱	lorg	erne /sta c/ca		
N/A	04-Dec-2024	5.5		M: fix ca	acheflus	h with	2 6 2 1 1	2108 6715 d384 2e28 f033	522a 153 8a43 ,	O-LIN-I 241224	
CVSSv3 Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	r 6-2	http:	5:// 7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It seems that the cacheflush syscall got broken when PAN for LPAE was implemented. User access was not enabled around the cache maintenance instructions, causing them to fault. CVE ID : CVE-2024-53137	git.kerne l.org/sta ble/c/e6 960a2ed 49c9a25 357817 535f7cc 50594a5 8604	
Affected Ver	sion(s): From (i	ncluding)	6.10.4 Up to (excluding) 6.11		
NULL Pointer Dereferenc e	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: avoid null_ptr_deref in vmw_framebuffer_surface_c reate_handle The 'vmw_user_object_buffer' function may return NULL with incorrect inputs. To avoid possible null pointer dereference, add a check whether the 'bo' is NULL in the vmw_framebuffer_surface_c reate_handle. CVE ID : CVE-2024-53115	https:// git.kerne l.org/sta ble/c/3 6f64da0 805551 75b58d 85f99f5f 90435e2 74e56, https:// git.kerne l.org/sta ble/c/9 3d1f41a 82de382 845af46 0bf03bc b17dcbf 08c5	O-LIN-LINU- 241224/1526
Affected Ver	sion(s): From (i	ncluding)	6.11 Up to (excluding) 6.11.10		
NULL Pointer Dereferenc e	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/3 6f64da0 805551	O-LIN-LINU- 241224/1527
			drm/vmwgfx: avoid null_ptr_deref in	75b58d 85f99f5f	

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vmw_framebuffer_surface_c reate_handle The 'vmw_user_object_buffer' function may return NULL with incorrect inputs. To avoid possible null pointer dereference, add a check whether the 'bo' is NULL in the vmw_framebuffer_surface_c reate_handle. CVE ID : CVE-2024-53115	90435e2 74e56, https:// git.kerne l.org/sta ble/c/9 3d1f41a 82de382 845af46 0bf03bc b17dcbf 08c5	
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: Revert "mmc: dw_mmc: Fix IDMAC operation with pages bigger than 4K" The commit 8396c793ffdf ("mmc: dw_mmc: Fix IDMAC operation with pages bigger than 4K") increased the max_req_size, even for 4K pages, causing various issues: - Panic booting the kernel/rootfs from an SD card on Rockchip RK3566 - Panic booting the kernel/rootfs from an SD card on StarFive JH7100 - "swiotlb buffer is full" and data corruption on StarFive JH7110	https:// git.kerne l.org/sta ble/c/0 0bff717 45bc358 3bd5ca5 9be91e0 ee1d27f 1944, https:// git.kerne l.org/sta ble/c/1 635e407 a4a64d0 8a8517a c59ca14 ad4fc78 5e75, https:// git.kerne l.org/sta ble/c/5 6de724c 58c07a7 ca3aac0 27cfd2c	O-LIN-LINU- 241224/1528

N/A04-Dec-20245.55.5Fix the following outer runtime PM protection "warning 1953.587208] (000:00:00:20: [drm] Missing outer runtime get noresu me+0x8d/0xa0 [xe]https:// git.kerne lorg/sta ble/c/c0 063108oLIN-LINU- ble/c/c0 06318N/A04-Dec-20245.55.50000:00:02.0: [drm] Missing outer runtime PM protection "warning 24>[953.587208] guc_exec_queue_fini+0x3a/ 0X4103 [xe]0-LIN-LINU- ble/c/c0 40384ce ecaefbea (782634 fcd3834 rad5180-LIN-LINU- ble/c/c0 40384ce ecaefbea (782634 fcd3834 rad518	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A 04-Dec-2024 5.5 In the Linux kernel, the following vulnerability has been resolved: N/A 04-Dec-2024 5.5 Is 7: Missing outer runtime PM protection "warning likerne Lorg/sta ble/c/c0 403e4ce ecaefbea f782633 [953.586396] xe 0641976 b. Fix the following outer runtime PM protection "warning likerne Lorg/sta ble/c/c0 403e4ce ecaefbea f782633 [953.586396] xe 0641976 b. Fix the following outer runtime PM protection "warning likerne Lorg/sta ble/c/c0 403e4ce ecaefbea f782633 [953.586396] xe 0641976 b. Fix the following outer runtime PM protection "warning likerne Lorg/sta ble/c/c0 403e4ce ecaefbea f782634 [953.587090] ? b. Fix the following outer runtime PM protection "warning likerne Lorg/sta ble/c/ed 782510 [953.587090] ? be/c/ed 78251719] guc_exec_queue_add_msg+0 2539ea4 440f8ad eeaa ecaefbea r2539ea4 r28/0x130 [xe] eea				been found, so it's probably better to just revert the change. This reverts commit 8396c793ffdf28bb8aee7cfe 0891080f8cab7890.		
N/A 04-Dec-2024 N/A 04-Dec-2024 I C C C C C C C C C C C C C C C C C C C				In the Linux kernel, the		
	N/A	04-Dec-2024	5.5	drm/xe/oa: Fix "Missing outer runtime PM protection" warning Fix the following drm_WARN: [953.586396] xe 0000:00:02.0: [drm] Missing outer runtime PM protection <4> [953.587090] ? xe_pm_runtime_get_noresu me+0x8d/0xa0 [xe] <4> [953.587208] guc_exec_queue_add_msg+0 x28/0x130 [xe] <4> [953.587319] guc_exec_queue_fini+0x3a/ 0x40 [xe] <4> [953.587425] xe_exec_queue_destroy+0xb	git.kerne l.org/sta ble/c/c0 403e4ce ecaefbea f78263d ffcd3e3f 06a19f6 b, https:// git.kerne l.org/sta ble/c/ed 7cd3510 d8da6e3 578d91 25a9ea4 440f8ad	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<4> [953.587515] xe_oa_release+0x9c/0xc0 [xe]		
			(cherry picked from commit b107c63d2953907908fd0c afb0e543b3c3167b75)		
Affected Ver	sion(s): From (i	ncluding	CVE ID : CVE-2024-53132 6.11.0 Up to (excluding) 6.11.1	0	
Allecteu veis		liciuuliigj	In the Linux kernel, the		
			following vulnerability has been resolved:	https:// git.kerne l.org/sta	
			vdpa: solidrun: Fix UB bug with devres	ble/c/0 b364cf5 3b2020 4e92bac	
			In psnet_open_pf_bar() and snet_open_vf_bar() a string later passed to	7c6ebd1 ee7d3ec 62931, https://	
			pcim_iomap_regions() is placed on the stack. Neither	git.kerne l.org/sta	
N/A	04-Dec-2024	7.8	pcim_iomap_regions() nor the functions it calls copy that string.	ble/c/5 bb287da 2d2d5b b8f7376 e223b02	O-LIN-LINU- 241224/1530
			Should the string later ever be used, this, consequently, causes	edb1699 8982e, https://	
			undefined behavior since the stack frame will by then have disappeared.	git.kerne l.org/sta ble/c/d 372dd0 9cfbf132	
			Fix the bug by allocating the strings on the heap through	4f54cbff d81fcaf6	
			devm_kasprintf().	cdf3e60 8e	
			CVE ID : CVE-2024-53126		

0-1

1-2

2-3

3-4 4-5 5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereferenc e	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/rockchip: vop: Fix a dereferenced before check warning The 'state' can't be NULL, we should check crtc_state. Fix warning: drivers/gpu/drm/rockchip /rockchip_drm_vop.c:1096 vop_plane_atomic_async_ch eck() warn: variable dereferenced before check 'state' (see line 1077) CVE ID : CVE-2024-53129	https:// git.kerne l.org/sta ble/c/1e 530597 29691ca 4d9051 18258b 9fbd17d 854174, https:// git.kerne l.org/sta ble/c/6 56dbd1c 21c2c08 8c70059 cdd43ec 83e7d54 ec4d, https:// git.kerne l.org/sta ble/c/ab 1c793f4 57f740a b7108cc 0b1340a 402dbf4 84d	O-LIN-LINU- 241224/1531
NULL Pointer Dereferenc e	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix null-ptr-deref in block_dirty_buffer tracepoint When using the "block:block_dirty_buffer" tracepoint, mark_buffer_dirty()	https:// git.kerne l.org/sta ble/c/2 026559a 6c4ce34 db117d 2db8f71 0fe2a94 20d5a, https:// git.kerne l.org/sta ble/c/7a	O-LIN-LINU- 241224/1532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may cause a NULL pointer dereference, or a general protection fault when KASAN is enabled. This happens because, since the tracepoint was added in	f3309c7 a2ef268 31a6712 5b11c34 a7e01c1 b2a, https:// git.kerne l.org/sta	
			mark_buffer_dirty(), it references the dev_t member bh->b_bdev- >bd_dev regardless of whether the buffer head has a pointer to	ble/c/8 6b1903 1dbc79a bc378df ae357f6	
			a block_device structure.	ea33ebe b0c95	
			implementation, nilfs_grab_buffer(), which grabs a buffer to read (or create) a block of metadata, including b-		
			tree node blocks, does not set the block device, but instead does so only if the buffer is		
			not in the "uptodate" state for each of its caller block reading functions. However, if the		
			uptodate flag is set on a folio/page, and the buffer heads are detached from it by		
			try_to_free_buffers(), and new buffer heads are then attached by create_empty_buffers(), the uptodate flag may		
CVSSv3 Scoring	Scale 0-1	1-2 2	- <mark>3 </mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be restored to each buffer without the block device being set to		
			bh->b_bdev, and mark_buffer_dirty() may be called later in that state,		
			resulting in the bug mentioned above.		
			Fix this issue by making nilfs_grab_buffer() always set the block device		
			of the super block structure to the buffer head, regardless of the state		
			of the buffer's uptodate flag.		
			CVE ID : CVE-2024-53130		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/0	
			nilfs2: fix null-ptr-deref in block_touch_buffer tracepoint	85556bf 8c70e26 29e02e7 9268dac 3016a08	
NULL Pointer Dereferenc e	04-Dec-2024	5.5	Patch series "nilfs2: fix null- ptr-deref bugs on block tracepoints".	b8bf, https:// git.kerne l.org/sta ble/c/3	O-LIN-LINU- 241224/1533
			This series fixes null pointer dereference bugs that occur when using nilfs2 and two block-related tracepoints.	b2a4fd9 bbee77a fdd3ed5 a05a0c0 2b6cde8 d3b9,	
			This patch (of 2):	https:// git.kerne l.org/sta ble/c/5	

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
			It has been reported that when using "block:block_touch_buffer" tracepoint, touch_buffer() called from nilfs_get_folio_block() causes a NULL pointer dereference, or a general protection fault when KASAN is	9b49ca6 7cca7b0 07a5afd 3de0283 c800815 7665	
			enabled.		
			This happens because since the tracepoint was added in touch_buffer(), it		
			references the dev_t member bh->b_bdev- >bd_dev regardless of whether the		
			buffer head has a pointer to a block_device structure. In the current		
			implementation, the block_device structure is set after the function		
			returns to the caller.		
			Here, touch_buffer() is used to mark the folio/page that owns the buffer		
			head as accessed, but the common search helper for folio/page used by the		
			caller function was optimized to mark the folio/page as accessed when it		

0-1

1-2

5-6

6-7

3-4

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was reimplemented a long time ago, eliminating the need to call		
			touch_buffer() here in the first place.		
			So this solves the issue by eliminating the touch_buffer() call itself.		
			CVE ID : CVE-2024-53131		
Affected Ver	sion(s): From (i	ncluding)	6.11.7 Up to (excluding) 6.11.2		
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	04-Dec-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: mm: revert "mm: shmem: fix data-race in shmem_getattr()" Revert d949d1d14fa2 ("mm: shmem: fix data-race in shmem_getattr()") as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over NFS. As Hugh commented, "added just to silence a syzbot sanitizer splat: added where there has never been any practical problem". CVE ID : CVE-2024-53136	https:// git.kerne l.org/sta ble/c/3 6b537e8 f302f67 0c7cf35 d88a3a2 94443e3 2d52, https:// git.kerne l.org/sta ble/c/5 874c115 0e77296 565ad6e 495ef41 fbf8757 0d14, https:// git.kerne l.org/sta ble/c/6 4e67e86 94252c1 bf01b80 2ee911b e3fee62 c36b	O-LIN-LINU- 241224/1534

0-1

1-2

Page 666 of 1137

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): From (i	ncluding)	6.12 Up to (excluding) 6.12.2	1	
N/A	06-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: add missing range check in bitmap_ip_uadt When tb[IPSET_ATTR_IP_TO] is not present but tb[IPSET_ATTR_CIDR] exists, the values of ip and ip_to are slightly swapped. Therefore, the range check for ip should be done later, but this part is missing and it seems that the vulnerability occurs. So we should add missing range checks and remove unnecessary range checks. CVE ID : CVE-2024-53141	https:// git.kerne l.org/sta ble/c/1 579483 5378ed5 6fb9bac c6a5dd3 b9f3352 0604e, https:// git.kerne l.org/sta ble/c/3 5f56c55 4eb1b56 b77b3cf 197a6b0 0922d4 9033d, https:// git.kerne l.org/sta ble/c/3c 20b594 8f119ae 61ee35a d8584d 666020c 91581	O-LIN-LINU- 241224/1535
Out-of- bounds Write	06-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: initramfs: avoid filename buffer overrun The initramfs filename field is defined in	https:// git.kerne l.org/sta ble/c/1a 423bbbe af9e3e2 0c46865 01efd9b 661fe83 4db, https:// git.kerne	O-LIN-LINU- 241224/1536

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Documentation/driver- api/early-userspace/buffer- format.rst as:	l.org/sta ble/c/4 9d01e73 6c30453	
			37 cpio_file := ALGN(4) + cpio_header + filename + "\0" + ALGN(4) + data	19e030d 1e75fb9 83011ab aca7,	
			 55 ======== ========================	https:// git.kerne l.org/sta ble/c/bb	
			==== 56 Field name Field size Meaning	7ac9667 0ab1d8d 681015f 9d66e45	
			57 ====== ==============================	dad579a f4d	
			 70 c_namesize 8 bytes Length of filename, including final \0		
			When extracting an initramfs cpio archive, the kernel's do_name() path		
			handler assumes a zero- terminated path at @collected, passing it		
			directly to filp_open() / init_mkdir() / init_mknod().		
			If a specially crafted cpio entry carries a non-zero- terminated filename		
			and is followed by uninitialized memory, then a file may be created with		

0-1

1-2

2-3

Page 668 of 1137

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trailing characters that represent the uninitialized memory. The ability		
			to create an initramfs entry would imply already having full control of		
			the system, so the buffer overrun shouldn't be considered a security		
			vulnerability.		
			Append the output of the following bash script to an existing initramfs		
			and observe any created /initramfs_test_fname_over runAA* path. E.g.		
			./reproducer.sh gzip >> /myinitramfs		
			It's easiest to observe non- zero uninitialized memory when the output is		
			gzipped, as it'll overflow the heap allocated @out_buf in gunzip(),		
			rather than the initrd_start+initrd_size block.		
			reproducer.sh		
			nilchar="A" # change to "\0" to properly zero terminate / pad		
			magic="070701"		
			ino=1		
			mode=\$((0100777)) uid=0		
CVSSv3 Scoring	Scale 0-1	1-2 2		6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gid=0		
			nlink=1		
			mtime=1		
			filesize=0		
			devmajor=0		
			devminor=1		
			rdevmajor=0		
			rdevminor=0		
			csum=0		
			fname="initramfs_test_fnam e_overrun"		
			namelen=\$((\${#fname} + 1)) # plus one to account for terminator		
			printf "%s%08x%08x%08x%08x %08x%08x%08x%08x%08 x%08x%08x%08x%08x%s " \ \$magic \$ino \$mode \$uid \$gid \$nlink \$mtime \$filesize \ \$devmajor \$devmajor \$devminor \$rdevmajor \$rdevminor \$namelen \$csum \$fname		
			<pre>termpadlen=\$((1 + ((4 - ((110 + \$namelen) & 3)) % 4))) printf "%.s\${nilchar}" \$(seq 1 \$termpadlen) reproducer.sh</pre>		

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

 *stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Symlink filename fields handled in do_symlink() won't overrun past the		
			data segment, due to the explicit zero-termination of the symlink		
			target.		
			Fix filename buffer overrun by aborting the initramfs FSM if any cpio		
			entry doesn't carry a zero- terminator at the expected (name_len - 1) offset.		
			CVE ID : CVE-2024-53142		
Affected Ver	sion(s): From (i	ncluding)	6.2 Up to (excluding) 6.6.63		
Use After Free	04-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: sctp: fix possible UAF in sctp_v6_available() A lockdep report [1] with CONFIG_PROVE_RCU_LIST= y hints that sctp_v6_available() is calling dev_get_by_index_rcu() and ipv6_chk_addr() without holding rcu. [1] ========	https:// git.kerne l.org/sta ble/c/0 5656a66 592759 242c740 636162 91b727 4d11b2f, https:// git.kerne l.org/sta ble/c/ad 975697 211f4f2c 4ce61c3 ba524fd 14d88ce ab8, https:// git.kerne l.org/sta ble/c/eb	O-LIN-LINU- 241224/1537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WARNING: suspicious RCU usage 6.12.0-rc5-virtme #1216 Tainted: G W net/core/dev.c:876 RCU- list traversed in non-reader section!!	72e7fcc 83987d 5d5595 b43222f 23b295 d5de7f	
			other info that might help us debug this:		
			rcu_scheduler_active = 2, debug_locks = 1		
			1 lock held by sctp_hello/31495:		
			<pre>#0: ffff9f1ebbdb7418 (sk_lock-AF_INET6){+.+.}- {0:0}, at: sctp_bind (./arch/x86/include/asm/j ump_label.h:27 net/sctp/socket.c:315) sctp</pre>		
			stack backtrace: CPU: 7 UID: 0 PID: 31495 Comm: sctp_hello Tainted: G W 6.12.0-rc5- virtme #1216 Tainted: [W]=WARN		
			Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian- 1.16.3-2 04/01/2014		
			Call Trace:		
			<task></task>		
			dump_stack_lvl (lib/dump_stack.c:123)		

4-5 5-6 6-7

7-8 8-9

9-10

2-3

1-2

0-1

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIP	CID
			lockdep_rcu_suspicious (kernel/locking/lockdep.c:6 822)			
			dev_get_by_index_rcu (net/core/dev.c:876 (discriminator 7))			
			sctp_v6_available (net/sctp/ipv6.c:701) sctp			
			sctp_do_bind (net/sctp/socket.c:400 (discriminator 1)) sctp			
			sctp_bind (net/sctp/socket.c:320) sctp			
			inet6_bind_sk (net/ipv6/af_inet6.c:465)			
			? security_socket_bind (security/security.c:4581 (discriminator 1))			
			sys_bind (net/socket.c:1848 net/socket.c:1869)			
			? do_user_addr_fault (./include/linux/rcupdate.h :347			
			 ./include/linux/rcupdate.h: 880 ./include/linux/mm.h:729 arch/x86/mm/fault.c:1340) 			
			? do_user_addr_fault (./arch/x86/include/asm/p reempt.h:84 (discriminator 13)			
			<pre>./include/linux/rcupdate.h: 98 (discriminator 13) /include/linux/rcupdate.h;</pre>			
			./include/linux/rcupdate.h:882 (discriminator 13)./include/linux/mm.h:729			
			(discriminator 13) arch/x86/mm/fault.c:1340			
			(discriminator 13))			
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
			x64_sys_bind (net/socket.c:1877 (discriminator 1) net/socket.c:1875 (discriminator 1) net/socket.c:1875 (discriminator 1)) do_syscall_64 (arch/x86/entry/common.c :52 (discriminator 1) arch/x86/entry/common.c: 83 (discriminator 1))		
			entry_SYSCALL_64_after_hw frame (arch/x86/entry/entry_64. S:130) RIP: 0033:0x7f59b934a1e7 Code: 44 00 00 48 8b 15 39 8c 0c 00 f7 d8 64 89 02 b8 ff ff ff ff eb bd 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 b8 31 00 00 00 0f 05 <48> 3d		
			01 f0 ff ff 73 01 c3 48 8b 0d 09 8c 0c 00 f7 d8 64 89 01 48 All code		
			0: 44 00 00 add %r8b,(%rax) 3: 48 8b 15 39 8c 0c 00		
			mov 0xc8c39(%rip),%rdx # 0xc8c43		
			a: f7 d8 neg %eax c: 64 89 02 mov %eax,%fs:(%rdx)		

4-5 5-6 6-7

7-8 8-9

9-10

0-1

1-2

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f: b8 ff ff ff ff mov \$0xffffffff,%eax		
			14: eb bd jmp 0xffffffffffffd3		
			16: 66 2e 0f 1f 84 00 00 cs nopw		
			0x0(%rax,%rax,1)		
			1d: 00 00 00		
			20: 0f 1f 00 nopl (%rax)		
			23: b8 31 00 00 00 mov \$0x31,%eax		
			28: 0f 05 syscall		
			2a:* 48 3d 01 f0 ff ff		
			cmp \$0xffffffffffffff001,%rax < trapping		
			instruction		
			30: 73 01 jae 0x33		
			32: c3 ret		
			33: 48 8b 0d 09 8c 0c 00 mov		
			0xc8c09(%rip),%rcx # 0xc8c43		
			3a: f7 d8 neg %eax		
			3c: 64 89 01 mov		
			%eax,%fs:(%rcx)		
			3f: 48 rex.W		
			Code starting with the faulting instruction		
			=		

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
			0: 48 3d 01 f0 ff ff cmp \$0xffffffffffffff001,%rax		
			6: 73 01 jae 0x9		
			8: c3 ret		
			9: 48 8b 0d 09 8c 0c 00		
			mov 0xc8c09(%rip),%rcx # 0xc8c19		
			10: f7 d8 neg %eax		
			12: 64 89 01 mov		
			%eax,%fs:(%rcx) 15: 48 rex.W		
			RSP: 002b:00007ffe2d0ad398 EFLAGS: 00000202 ORIG_RAX: 000000000000031		
			RAX: fffffffffffffffda RBX: 00007ffe2d0ad3d0 RCX: 00007f59b934a1e7		
			RDX: 0000000000000001c RSI: 00007ffe2d0ad3d0 RDI: 00000000000000005		
			RBP: 00000000000000005 R08: 19999999999999999 R09: 000000000000000000		
			R10: 00007f59b9253298 R11: 000000000000		
			truncated		
			CVE ID : CVE-2024-53139		
N/A	04-Dec-2024	6.5	In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/aa 0d42cac	O-LIN-LINU- 241224/1538

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
			KVM: VMX: Bury Intel PT virtualization (guest/host mode) behind CONFIG_BROKEN	f093a6fc ca872ed c954f6f8 12926a1 7,	
			Hide KVM's pt_mode module param behind CONFIG_BROKEN, i.e. disable support for virtualizing Intel PT via guest/host mode unless BROKEN=y. There are	https:// git.kerne l.org/sta ble/c/b 91bb0ce 5cd7005 b376eac 690ec66 4c1b563	
			myriad bugs in the implementation, some of which are fatal to the guest,	72ec, https:// git.kerne	
			and others which put the stability and health of the host at risk.	l.org/sta ble/c/d 28b059e e4779b5	
			For guest fatalities, the most glaring issue is that KVM fails to ensure	102c5da 6e92976 252051 0e406	
			tracing is disabled, and *stays* disabled prior to VM-Enter, which is	00400	
			necessary as hardware disallows loading (the guest's) RTIT_CTL if tracing		
			is enabled (enforced via a VMX consistency check). Per the SDM:		
			If the logical processor is operating with Intel PT enabled (if		
			IA32_RTIT_CTL.TraceEn = 1) at the time of VM entry, the "load		

0-1

1-2

2-3

3-4 4-5 5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IA32_RTIT_CTL" VM-entry control must be 0.		
			On the host side, KVM doesn't validate the guest CPUID configuration		
			provided by userspace, and even worse, uses the guest configuration to		
			decide what MSRs to save/load at VM-Enter and VM-Exit. E.g. configuring		
			guest CPUID to enumerate more address ranges than are supported in hardware		
			will result in KVM trying to passthrough, save, and load non-existent MSRs,		
			which generates a variety of WARNs, ToPA ERRORs in the host, a potential		
			deadlock, etc.		
			CVE ID : CVE-2024-53135		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/0a	
			vp_vdpa: fix id_table array not null terminated error	886489 d27459 6ad1a80 789d3a7	
N/A	02-Dec-2024	5.5	Allocate one extra virtio_device_id as null terminator, otherwise	735032 10a615, https:// git.kerne	O-LIN-LINU- 241224/1539
			vdpa_mgmtdev_get_classes() may iterate multiple times and visit	l.org/sta ble/c/4e 39ecadf	
			undefined memory.	1d2a081 871396	
			CVE ID : CVE-2024-53110	19f1f31	
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
				4b64ba7 d947, https:// git.kerne l.org/sta ble/c/8 70d68fe 17b5d9 032049 dcad98b 5781a34 4a8657	
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ocfs2: uncache inode which has failed entering the group Syzbot has reported the following BUG: kernel BUG at fs/ocfs2/uptodate.c:509! Call Trace: <task> ?die_body+0x5f/0xb0 ? die+0x9e/0xc0 ? do_trap+0x15a/0x3a0 ? ocfs2_set_new_buffer_uptod ate+0x145/0x160 ? do_error_trap+0x1dc/0x2c 0</task>	https:// git.kerne l.org/sta ble/c/6 20d225 98110b 0d0cb97 a3fcca65 fc473ea 86e73, https:// git.kerne l.org/sta ble/c/7 37f3413 7844d6 572ab7d 473c998 c7f977ff 30eb, https:// git.kerne l.org/sta ble/c/8 43dfc80 4af4b33 8ead423 31dd58 081b42 8ecdf8	O-LIN-LINU- 241224/1540

0-1

1-2

3-4 4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? ocfs2_set_new_buffer_uptod ate+0x145/0x160 ?		
			pfx_do_error_trap+0x10/0 x10		
			? handle_invalid_op+0x34/0x 40		
			? ocfs2_set_new_buffer_uptod ate+0x145/0x160		
			? exc_invalid_op+0x38/0x50		
			? asm_exc_invalid_op+0x1a/0 x20		
			? ocfs2_set_new_buffer_uptod ate+0x2e/0x160		
			? ocfs2_set_new_buffer_uptod ate+0x144/0x160		
			? ocfs2_set_new_buffer_uptod ate+0x145/0x160		
			ocfs2_group_add+0x39f/0x 15a0		
			? pfx_ocfs2_group_add+0x1 0/0x10		
			? pfx_lock_acquire+0x10/0x 10		
			? mnt_get_write_access+0x68 /0x2b0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? pfx_lock_release+0x10/0x 10		
			? rcu_read_lock_any_held+0x b7/0x160		
			? pfx_rcu_read_lock_any_hel		
			d+0x10/0x10 ? smack_log+0x123/0x540		
			? mnt_get_write_access+0x68 /0x2b0		
			? mnt_get_write_access+0x68 /0x2b0		
			? mnt_get_write_access+0x22 6/0x2b0		
			ocfs2_ioctl+0x65e/0x7d0 ?		
			? pfx_ocfs2_ioctl+0x10/0x1 0		
			? smack_file_ioctl+0x29e/0x3 a0		
			? pfx_smack_file_ioctl+0x10 /0x10		
			? lockdep_hardirqs_on_prepa re+0x43d/0x780		
			? pfx_lockdep_hardirqs_on_ prepare+0x10/0x10		
			? pfx_ocfs2_ioctl+0x10/0x1 0		
			se_sys_ioctl+0xfb/0x170		
CVSSv3 Scoring *stands for all v		1-2 2	- 3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Descrip	tion & C	/E ID	Pa	tch	NCIIF	C ID
			do_syscall_ entry_SYSC			7			
			frame+0x72			V			
			When 'ioctl(OCFS DD,)' has particular						
			inode in 'ocfs2_verif ut()', corres head		-)			
			remains cao subsequent 'ioctl()' for	t call to t	he same				
			inode issue 'ocfs2_set_r date()' (tryi	new_buff	0				
			to cache the head of that by uncachir	t inode).					
			the buffer h 'ocfs2_remo)' on error p	ove_from					
			'ocfs2_grou	p_add()					
			CVE ID : CV	/E-2024	-53112				
NULL			In the Linux following vi been resolv	ulnerabi		git.k l.org ble/			
Pointer Dereferenc e	02-Dec-2024	5.5	mm: fix NU dereference alloc_pages	e in		ec3 dbd 004	7ba9 e710 0bb 57cc	O-LIN-L 241224	
						6d2 http	c19, s://		
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

			We triggered a NULL pointer dereference for ac.preferred_zoneref->zone in	git.kerne l.org/sta ble/c/6a ddb2d9	
			alloc_pages_bulk_noprof() when the task is migrated between cpusets.	501ec86 6d7b3a3 b4e6653 07c437e 9be2,	
			When cpuset is enabled, in prepare_alloc_pages(), ac- >nodemask may be	https:// git.kerne l.org/sta ble/c/8c	
			¤t->mems_allowed. when first_zones_zonelist() is called to find	e41b0f9 d77cca0 74df25a	
			preferred_zoneref, the ac- >nodemask may be modified concurrently if the task is migrated between	fd39b86 e2ee3aa 68e	
			different cpusets. Assuming we have 2 NUMA Node, when traversing Node1 in		
			ac->zonelist, the nodemask is 2, and when		
			traversing Node2 in ac- >zonelist, the nodemask is 1. As a result, the		
			ac->preferred_zoneref points to NULL zone.		
			In alloc_pages_bulk_noprof(), for_each_zone_zonelist_nod emask() finds a		
			allowable zone and calls zonelist_node_idx(ac.prefer red_zoneref), leading		
			to NULL pointer dereference.		
CVSSv3 Scoring S	cale 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
			alloc_pages_noprof() fixes this issue by checking NULL pointer in commit		
			ea57485af8f4 ("mm, page_alloc: fix check for NULL preferred_zone") and		
			commit df76cee6bbeb ("mm, page_alloc: remove redundant checks from alloc		
			fastpath").		
			To fix it, check NULL pointer for preferred_zoneref->zone.		
			CVE ID : CVE-2024-53113	http://	
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/2	
			virtio/vsock: Fix accept_queue memory leak	415345 042245 de7601d cc6eafdb	
Missing Release of			As the final stages of socket destruction may be delayed, it is possible	e3a3dcc 9e379, https:// git.kerne	
Memory after Effective Lifetime	02-Dec-2024	5.5	that virtio_transport_recv_listen () will be called after the accept_queue	l.org/sta ble/c/8 97617a4 13e0bf1	O-LIN-LINU- 241224/1542
			has been flushed, but before the SOCK_DONE flag has been set. As a result,	c6380e3 b34b2f2 8f45050 8549,	
			sockets enqueued after the flush would remain unremoved, leading to a	https:// git.kerne l.org/sta	
			memory leak.	ble/c/9 46c7600	
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	fa2207c	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vsock_release	c8d3fbc	
			vsock_release	86a518e c56f98a	
			lock	5813	
			virtio_transport_release		
			virtio_transport_close		
			schedule_delayed_work(clo se_work)		
			sk_shutdown = SHUTDOWN_MASK		
			(!) flush accept_queue		
			release		
			virtio_transport_recv_pkt		
			vsock_find_bound_socket		
			lock		
			if flag(SOCK_DONE) return		
			virtio_transport_recv_listen child		
			= vsock_create_connected		
			(!) vsock_enqueue_accept(child)		
			release		
			close_work		
			lock		
			virtio_transport_do_close		
			set_flag(SOCK_DONE)		
			virtio_transport_remove_so ck		
			vsock_remove_sock		

4-5

5-6

6-7

7-8

8-9

9-10

3-4

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vsock_remove_bound		
			release		
			Introduce a sk_shutdown		
			check to disallow vsock_enqueue_accept()		
			during		
			socket destruction.		
			unreferenced object		
			0xffff888109e3f800 (size 2040):		
			comm "kworker/5:2", pid 371, jiffies 4294940105		
			hex dump (first 32 bytes):		
			00 00 00 00 00 00 00 00 00 00 00 00 00 0		
			28 00 0b 40 00 00 00 00		
			00 00 00 00 00 00 00 00 00 (@		
			backtrace (crc 9e5f4e84):		
			[<fffffff81418ff1>]</fffffff81418ff1>		
			kmem_cache_alloc_noprof+ 0x2c1/0x360		
			[<ffffffff81d27aa0>] sk_prot_alloc+0x30/0x120</ffffffff81d27aa0>		
			[<ffffffff81d2b54c>] sk_alloc+0x2c/0x4b0</ffffffff81d2b54c>		
			[<fffffff81fe049a>]</fffffff81fe049a>		
			vsock_create.constprop.0+ 0x2a/0x310		
			[<fffffff81fe6d6c>]</fffffff81fe6d6c>		
			virtio_transport_recv_pkt+0 x4dc/0x9a0		
			[<fffffffff81fe745d>] vsock_loopback_work+0xfd</fffffffff81fe745d>		
			/0x140		
CVSSv3 Scoring		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
			[<fffffff810fc6ac>] process_one_work+0x20c/0 x570</fffffff810fc6ac>		
			[<ffffffff810fce3f>] worker_thread+0x1bf/0x3a 0</ffffffff810fce3f>		
			[<ffffffff811070dd>] kthread+0xdd/0x110</ffffffff811070dd>		
			[<ffffffff81044fdd>] ret_from_fork+0x2d/0x50</ffffffff81044fdd>		
			[<ffffffff8100785a>] ret_from_fork_asm+0x1a/0 x30</ffffffff8100785a>		
			CVE ID : CVE-2024-53119		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/0	
			net/mlx5e: CT: Fix null-ptr- deref in add rule err flow	6dc488a 593020 bd2f006 798557	
			In error flow of mlx5_tc_ct_entry_add_rule() , in case ct_rule_add()	d2a3210 4d8359, https:// git.kerne	
NULL Pointer Dereferenc	02-Dec-2024	5.5	callback returns error, zone_rule->attr is used uninitiated. Fix it to	l.org/sta ble/c/0c 7c70ff8b	O-LIN-LINU- 241224/1543
e			use attr which has the needed pointer value.	696cfed ba35041 1dca736 361ef9a	
			Kernel log:	0f,	
			BUG: kernel NULL pointer dereference, address: 000000000000110	https:// git.kerne l.org/sta	
			RIP: 0010:mlx5_tc_ct_entry_add_ rule+0x2b1/0x2f0	ble/c/6 030f8bd 7902e9e	
			[mlx5_core]	276a0ed c09bf11	

CVSSv3 Scoring Scale0-11-22-33-44-55-66-7*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				979e4e2	
			Call Trace:	bc2e	
			<task></task>		
			?_die+0x20/0x70		
			?		
			page_fault_oops+0x150/0x 3e0		
			?		
			exc_page_fault+0x74/0x140		
			?		
			asm_exc_page_fault+0x22/0 x30		
			?		
			mlx5_tc_ct_entry_add_rule+ 0x2b1/0x2f0 [mlx5_core]		
			?		
			mlx5_tc_ct_entry_add_rule+		
			0x1d5/0x2f0 [mlx5_core]		
			mlx5_tc_ct_block_flow_offlo		
			ad+0xc6a/0xf90		
			[mlx5_core]		
			? nf_flow_offload_tuple+0xd8		
			/0x190 [nf_flow_table]		
			nf_flow_offload_tuple+0xd8 /0x190 [nf_flow_table]		
			/ ovr >o [m_now_cone]		
			flow_offload_work_handler+		
			0x142/0x320		
			[nf_flow_table]		
			? finish_task_switch.isra.0+0x		
			15b/0x2b0		
			process_one_work+0x16c/0 x320		
			AJ20		

0-1

1-2

Page **688** of **1137**

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Concurrent Execution using Shared Resource Condition)Isoapper Leverable Concurrent Such and Shared ConditionIsoapper Leverable Such and Shared Concurrent Such and Shared ConditionIsoapper Leverable Such and Shared ConditionIsoapper Leverable Such and Shared Concurrent Such and Shared ConditionIsoapper Leverable Such and Shared Concurrent Such and Shared Concurrent Such and Shared Concurrent Concurrent Shared Resource ConditionIsoapper Such and Shared Such and Shared Concurrent Such and Shared ConditionIsoapper Such and Shared Such and Shared Such and Shared ConditionIsoapper Such and Shared Such and Shared Such and Shared Shared ConditionIsoapper Such and Shared Such and Shared Such and Shared Such and Shared ConditionIsoapper Such and Shared Such and Shared Such and Shared Such and Shared ConditionIsoapper Such and Shared Shared Such and Shared Such and Shared Such and Shared Shared ConditionIsoapper Such and Shared S	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with [TRace Condition]In the Linux kernel, the following vulnerability has been resolved:https:// git.kerne l.org/sta ble/c/0 94d1a21 21ce1 85ab07d 7438869https:// git.kerne l.org/sta ble/c/0 94d1a21 21ce1 85ab07d 7438869https:// 9409dcf b5b9, https:// git.kerne l.org/sta ble/c/0 94d1a21 21ce1 85ab07d 7012b6https:// 9409dcf b5b9, https:// git.kerne l.org/sta ble/c/0 9401a21 21ce1 85ab07d 7012b6O-LIN-LINU- 241224/1544 ble/c/9 a3ef0d1 7012b6 53e9e60 06e3f50 coditionCondition'0-LIN-LINU- 241224/1544 ble/c/9 a3ef0d1 rom hardware, set the hardware deletion function to NULL and unlock the group, delet the software copy of the FTE, and git.kerne to NULL and unlock the process for deleting FTEs.0-LIN-LINU- 241224/1544 ble/c/9 a3ef0d1 7012b6 53e9e60 06e3f50 code3f50 cogroup, delet the software copy of the FTE, and git.kerne to remove it from the xarray.				<pre>worker_thread+0x28c/0x3a 0 ?pfx_worker_thread+0x10/ 0x10 kthread+0xb8/0xf0 ?pfx_kthread+0x10/0x10 ret_from_fork+0x2d/0x50 ?pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0</pre>		
Image: constraint of the constra						
Concurrent Execution using Shared Resource with02-Dec-20245.55.5in the bind kterne, the following vulnerability has been resolved:git.kerne lorg/sta ble/c/0 94d1a21 21cee1e 85ab07d 4809dcf b5b9, https:// git.kerne https:// git.kerne https:// git.kerne https:// git.kerne https:// 241224/1544Condition')02-Dec-20245.5- Lock the FTE, delete it from hardware, set the hardware deletion function 53e9e60 to NULL and unlock the FTE.0-LIN-LINU- 241224/1544Condition')- Lock the parent flow group, delete the software copy of the FTE, and git.kerne Lorg/sta0-LIN-LINU- 241224/1544						
	Execution using Shared Resource with Improper Synchroniz ation ('Race	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: fs, lock FTE when checking if active The referenced commits introduced a two-step process for deleting FTEs: - Lock the FTE, delete it from hardware, set the hardware deletion function to NULL and unlock the FTE. - Lock the parent flow group, delete the software copy of the FTE, and	git.kerne l.org/sta ble/c/0 94d1a21 21cee1e 85ab07d 74388f9 4809dcf b5b9, https:// git.kerne l.org/sta ble/c/9 33ef0d1 7f012b6 53e9e60 06e3f50 c8d0238 b5ed, https:// git.kerne l.org/sta	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			However, this approach encounters a race condition if a rule with the same match value is added simultaneously. In this scenario, fs_core may set the hardware deletion function	a314419 930f913 5727e39 d77e662 62d5f7b ef6	
			to NULL prematurely, causing a panic during		
			subsequent rule deletions.		
			To prevent this, ensure the active flag of the FTE is checked under a lock,		
			which will prevent the fs_core layer from attaching a new steering rule to		
			an FTE that is in the process of deletion.		
			[438.967589] MOSHE: 2496 mlx5_del_flow_rules del_hw_func		
			[438.968205][cut here]		
			[438.968654] refcount_t: decrement hit 0; leaking memory.		
			[438.969249] WARNING: CPU: 0 PID: 8957 at lib/refcount.c:31 refcount_warn_saturate+0xf b/0x110		
			[438.970054] Modules linked in: act_mirred cls_flower act_gact sch_ingress openvswitch		

Page 690 of 1137

4-5

5-6

6-7

7-8

8-9

9-10

3-4

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nsh mlx5_vdpa vringh vhost_iotlb vdpa mlx5_ib mlx5_core xt_conntrack xt_MASQUERADE nf_conntrack_netlink nfnetlink xt_addrtype iptable_nat nf_nat br_netfilter rpcsec_gss_krb5 auth_rpcgss oid_registry overlay rpcrdma rdma_ucm ib_iser libiscsi scsi_transport_iscsi ib_umad rdma_cm ib_ipoib iw_cm ib_cm ib_uverbs ib_core zram zsmalloc fuse [last unloaded: cls_flower]	Fatch	
			[438.973288] CPU: 0 UID: 0 PID: 8957 Comm: tc Not tainted 6.12.0-rc1+ #8 [438.973888] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0- gf21b5a4aeb02- prebuilt.qemu.org 04/01/2014		
			[438.974874] RIP: 0010:refcount_warn_satura te+0xfb/0x110		
			[438.975363] Code: 40 66 3b 82 c6 05 16 e9 4d 01 01 e8 1f 7c a0 ff 0f 0b c3 cc cc cc cc 48 c7 c7 10 66 3b 82 c6 05 fd e8 4d 01 01 e8 05 7c a0 ff <0f> 0b c3 cc cc cc cc 66 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 90		
			[438.976947] RSP: 0018:ffff888124a53610 EFLAGS: 00010286		
			[438.977446] RAX: 0000000000000000 RBX:		
CVSSv3 Scoring *stands for all v		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
			ffff888119d56de0 RCX: 0000000000000000		
			[438.978090] RDX: ffff88852c828700 RSI: ffff88852c81b3c0 RDI: ffff88852c81b3c0		
			[438.978721] RBP: ffff888120fa0e88 R08: 0000000000000000 R09: ffff888124a534b0		
			[438.979353] R10: 0000000000000001 R11: 0000000000000001 R12: ffff888119d56de0		
			[438.979979] R13: ffff888120fa0ec0 R14: ffff888120fa0ee8 R15: ffff888119d56de0		
			[438.980607] FS: 00007fe6dcc0f800(0000) GS:ffff88852c800000(0000) knlGS:00000000000000000		
			[438.983984] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033		
			[438.984544] CR2: 00000000004275e0 CR3: 0000000186982001 CR4: 000000000372eb0		
			[438.985205] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 00000000000000000		
			[438.985842] DR3: 0000000000000000 DR6: 000000000fffe0ff0 DR7: 00000000000000400		
			[438.986507] Call Trace:		
			[438.986799] <task></task>		

0-1

1-2

3-4 4-5 5-6

7-8 8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<pre>[438.987070] ?warn+0x7d/0x110 [438.987426] ? refcount_warn_saturate+0xf b/0x110</pre>		
			/ [438.987877] ? report_bug+0x17d/0x190		
			[438.988261] ? prb_read_valid+0x17/0x20		
			[438.988659] ? handle_bug+0x53/0x90		
			[438.989054] ? exc_invalid_op+0x14/0x70		
			[438.989458] ? asm_exc_invalid_op+0x16/0 x20		
			[438.989883] ? refcount_warn_saturate+0xf b/0x110		
			[438.990348] mlx5_del_flow_rules+0x2f7/ 0x340 [mlx5_core]		
			[438.990932] mlx5_eswitch_del_rule+0x 49/0x170 [mlx5_core]		
			[438.991519] ? mlx5_lag_is_sriov+0x3c/0x5 0 [mlx5_core]		
			[438.992054] ? xas_load+0x9/0xb0		
			[438.992407] mlx5e_tc_rule_unoffload+0x 45/0xe0 [mlx5_core]		
			[438.993037] mlx5e_tc_del_fdb_flow+0x2 a6/0x2e0 [mlx5_core]		
			[438.993623] mlx5e_flow_put+0x29/0x60 [mlx5_core]		
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
			[438.994161] mlx5e_delete_flower+0x261 /0x390 [mlx5_core]		
			[438.994728] tc_setup_cb_destroy+0xb9/ 0x190		
			[438.995150] fl_hw_destroy_filter+0x94/ 0xc0 [cls_flower]		
			[438.995650] fl_change+0x11a4/0x13c0 [cls_flower]		
			[438.996105] tc_new_tfilter+0x347/0xbc0		
			[438.996503] ?		
			truncated		
			CVE ID : CVE-2024-53121		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/2	
Concurrent Execution using			mptcp: cope racing subflow creation in mptcp_rcv_space_adjust	499585 1d58c4a 205ad0f fa7b2f2 1e479a9	
Shared Resource with	02-Dec-2024	5.5	Additional active subflows - i.e. created by the in kernel path	c8527, https:// git.kerne l.org/sta	O-LIN-LINU- 241224/1545
Improper Synchroniz ation ('Race			manager - are included into the subflow list before starting the	ble/c/aa d6412c6 3baa39d	,
Condition')			3whs.	d813e81	
				f16a14d 976b3de	
			A racing recvmsg() spooling	2e8,	
			data received on an already established	https://	
			subflow would	git.kerne l.org/sta	
			unconditionally call	ble/c/ce	

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tcp_cleanup_rbuf() on all the current subflows, potentially hitting a divide by zero error on the newly created ones. Explicitly check that the subflow is in a suitable state before invoking tcp_cleanup_rbuf().	7356ae3 5943cc6 494cc69 2e62d51 a734062 b7d	
			CVE ID : CVE-2024-53122		
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: kTLS, Fix incorrect page refcounting The kTLS tx handling code is using a mix of get_page() and page_ref_inc() APIs to increment the page reference. But on the release path (mlx5e_ktls_tx_handle_resy nc_dump_comp()), only put_page() is used. This is an issue when using pages from large folios: the get_page()	https:// git.kerne l.org/sta ble/c/2 723e8b2 cbd486c b96e5a6 1b2247 3f7fd62 e18df, https:// git.kerne l.org/sta ble/c/6 9fbd07f 17b0fda f8970bc 705f5bf 115c297 839d, https:// git.kerne l.org/sta ble/c/9	O-LIN-LINU- 241224/1546
			references are stored on the folio page while the page_ref_inc()	3a14620 b97c911 489a5b0 08782f3	

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
			references are stored directly in the given page. On release the folio page will be dereferenced too many times.	d9b0c4a eff4	
			This was found while doing kTLS testing with sendfile() + ZC when the served file was read from NFS on a kernel with NFS		
			large folios support (commit 49b29a573da8 ("nfs: add support for large folios")).		
N/A	04-Dec-2024	5.5	CVE ID : CVE-2024-53138 In the Linux kernel, the following vulnerability has been resolved: netlink: terminate outstanding dump on socket close Netlink supports iterative dumping of data. It provides the families the following ops: - start - (optional) kicks off the dumping process - dump - actual dump helper, keeps getting called until it returns 0 - done - (optional) pairs with .start, can be used for cleanup	https:// git.kerne l.org/sta ble/c/1 14a61d8 d94ae3a 43b824 46cf737f d75702 1b834, https:// git.kerne l.org/sta ble/c/1 76c41b3 ca9281a 9736b6 7c6121b 03dbf0c 8c08f, https:// git.kerne l.org/sta ble/c/1 904fb9e bf91144	O-LIN-LINU- 241224/1547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC	ID
			The whole process is asynchronous and the repeated calls to .dump don't actually happen in a tight loop, but rather are triggered	1f90a68 e96b22a a73e441 0505		
			in response to recvmsg() on the socket.			
			This gives the user full control over the dump, but also means that			
			the user can close the socket without getting to the end of the dump.			
			To make sure .start is always paired with .done we check if there			
			is an ongoing dump before freeing the socket, and if so call .done.			
			The complication is that sockets can get freed from BH and .done			
			is allowed to sleep. So we use a workqueue to defer the call, when			
			needed.			
			Unfortunately this does not work correctly. What we defer is not			
			the cleanup but rather releasing a reference on the socket.			
			We have no guarantee that we own the last reference, if someone			
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		
			else holds the socket they may release it in BH and we're back				
			to square one.				
			The whole dance, however, appears to be unnecessary. Only the user				
			can interact with dumps, so we can clean up when socket is closed.				
			And close always happens in process context. Some async code may				
			still access the socket after close, queue notification skbs to it etc.				
			but no dumps can start, end or otherwise make progress.				
			Delete the workqueue and flush the dump state directly from the release				
			handler. Note that further cleanup is possible in -next, for instance				
			we now always call .done before releasing the main module reference,				
			so dump doesn't have to take a reference of its own.				
			CVE ID : CVE-2024-53140				
	sion(s): From (i	ncluding)	6.5.9 Up to (excluding) 6.6				
Concurrent Execution using Shared Resource	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/5 813022	O-LIN-LINU- 241224/1548		
CVSSv3 Scoring	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
with			mptcp: error out earlier on	98524e9	
Improper			disconnect	d77c4c4	
Synchroniz				4ff5156	
ation			Eric reported a division by	a6cd112	
('Race			zero splat in the MPTCP	227ae,	
Condition')			protocol:	https:// git.kerne	
				l.org/sta	
				ble/c/9	
			Oops: divide error: 0000	55388e1	
			[#1] PREEMPT SMP KASAN PTI	d5d222c	
				4101c59	
			CPU: 1 UID: 0 PID: 6094	6b536d	
			Comm: syz-executor317	41b91a8	
			Not tainted	b212e,	
			6.12.0-rc5-syzkaller-00291-	https://	
			g05b92660cdfe #0	git.kerne	
			Hardware name: Google	l.org/sta	
			Google Compute	ble/c/a6	
			Engine/Google Compute	6805c9b	
			Engine,	22caf4e	
			BIOS Google 09/13/2024	42af7a6 16f6c6b	
			RIP:	83c90d1	
			0010:tcp_select_window+	010	
			0x5b4/0x1310	010	
			net/ipv4/tcp_output.c:3163		
			Code: f6 44 01 e3 89 df e8		
			9b 75 09 f8 44 39 f3 0f 8d		
			11 ff ff ff e8		
			0d 74 09 f8 45 89 f4 e9 04 ff		
			ff ff e8 00 74 09 f8 44 89 f0		
			99 <f7> 7c</f7>		
			24 14 41 29 d6 45 89 f4 e9 ec fe ff ff e8 e8 73 09 f8 48		
			89		
			RSP:		
			0018:ffffc900041f7930		
			EFLAGS: 00010293		
			RAX: 000000000017e67		
			RBX: 000000000017e67		
			RCX: ffffffff8983314b		
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 ve					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RDX: 0000000000000000 RSI: fffffff898331b0 RDI: 00000000000000004		
			RBP: 00000000005d6000 R08: 0000000000000004 R09: 0000000000017e67		
			R10: 000000000003e80 R11: 0000000000000000 R12: 000000000003e80		
			R13: ffff888031d9b440 R14: 0000000000017e67 R15: 00000000002eb000		
			FS: 00007feb5d7f16c0(0000) GS:ffff8880b8700000(0000		
) knlGS:0000000000000000000		
			CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033		
			CR2: 00007feb5d8adbb8 CR3: 0000000074e4c000 CR4: 00000000003526f0		
			DR0: 00000000000000000 DR1: 00000000000000000 DR2: 0000000000000000000		
			DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 000000000000000400		
			Call Trace:		
			<task></task>		
			tcp_cleanup_rbuf+0x3e7/ 0x4b0 net/ipv4/tcp.c:1493		
			mptcp_rcv_space_adjust net/mptcp/protocol.c:2085 [inline]		
			mptcp_recvmsg+0x2156/0x 2600 net/mptcp/protocol.c:2289		

4-5 5-6 6-7

7-8 8-9

9-10

0-1

1-2

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inet_recvmsg+0x469/0x6a0 net/ipv4/af_inet.c:885		
			sock_recvmsg_nosec net/socket.c:1051 [inline]		
			sock_recvmsg+0x1b2/0x25 0 net/socket.c:1073		
			sys_recvfrom+0x1a5/0x2 e0 net/socket.c:2265		
			do_sys_recvfrom net/socket.c:2283 [inline]		
			se_sys_recvfrom net/socket.c:2279 [inline]		
			x64_sys_recvfrom+0xe0/0 x1c0 net/socket.c:2279		
			do_syscall_x64 arch/x86/entry/common.c: 52 [inline]		
			do_syscall_64+0xcd/0x250 arch/x86/entry/common.c: 83		
			entry_SYSCALL_64_after_hw frame+0x77/0x7f	T	
			RIP: 0033:0x7feb5d857559		
			Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 51 18 00 00 90 48 89 f8 48		
			89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d		
			01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48		
			RSP: 002b:00007feb5d7f1208 EFLAGS: 00000246 ORIG_RAX: 00000000000002d		
			RAX: fffffffffffffffda RBX: 00007feb5d8e1318 RCX: 00007feb5d857559		
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
			RDX: 000000800000000 RSI: 0000000000000000 RDI: 00000000000000003		
			RBP: 00007feb5d8e1310 R08: 00000000000000000 R09: ffffffff81000000		
			R10: 00000000000000100 R11: 0000000000000246 R12: 00007feb5d8e131c		
			R13: 00007feb5d8ae074 R14: 000000800000000e R15: 00000000fffffdef		
			and provided a nice reproducer.		
			The root cause is the current bad handling of racing disconnect.		
			After the blamed commit below, sk_wait_data() can return (with		
			error) with the underlying socket disconnected and a zero rcv_mss.		
			Catch the error and return without performing any additional		
			operations on the current socket.		
Affected Ver	sion(s): From (i	ncluding	CVE ID : CVE-2024-53123 6.6 Up to (excluding) 6.6.63		
Aniceleu vel		neruunigj	or of the ferending 0.0.03	https://	
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	git.kerne l.org/sta ble/c/2 47d720 b2c5d22	O-LIN-LINU- 241224/1549
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
			nommu: pass NULL argument to vma_iter_prealloc()	f728143 7fd6054 a138256 986ba,	
			When deleting a vma entry from a maple tree, it has to pass NULL to	https:// git.kerne l.org/sta ble/c/8	
			vma_iter_prealloc() in order to calculate internal state of the tree, but	bbf0ab6 31cdf1d ade6745	
			it passed a wrong argument. As a result, nommu kernels crashed upon	f137cff9 8751e6c ed7,	
			accessing a vma iterator, such as acct_collect() reading the size of vma	https:// git.kerne l.org/sta ble/c/ac	
			entries after do_munmap().	eaf33b7 666b72 dfb86e0	
			This commit fixes this issue by passing a right argument to the	aa977be 81e3bcb c727	
			preallocation call. CVE ID : CVE-2024-53109		
Concurrent Execution			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/5	
using Shared Resource	using Shared Resource with 02-Dec-2024 Improper Synchroniz ation	02-Dec-2024 5.5	mptcp: error out earlier on disconnect	813022 98524e9 d77c4c4 4ff5156	O-LIN-LINU-
with Improper Synchroniz ation ('Race			Eric reported a division by zero splat in the MPTCP protocol:	a6cd112 227ae, https:// git.kerne	241224/1550
Condition')			Oops: divide error: 0000 [#1] PREEMPT SMP KASAN PTI	l.org/sta ble/c/9 55388e1 d5d222c 4101c59	

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CPU: 1 UID: 0 PID: 6094 Comm: syz-executor317 Not tainted	6b536d 41b91a8 b212e,	
			6.12.0-rc5-syzkaller-00291- g05b92660cdfe #0	https:// git.kerne	
			Hardware name: Google Google Compute Engine/Google Compute Engine,	l.org/sta ble/c/a6 6805c9b 22caf4e 42af7a6	
			BIOS Google 09/13/2024	16f6c6b 83c90d1	
			RIP: 0010:tcp_select_window+ 0x5b4/0x1310 net/ipv4/tcp_output.c:3163	010	
			Code: f6 44 01 e3 89 df e8 9b 75 09 f8 44 39 f3 0f 8d 11 ff ff ff e8		
			0d 74 09 f8 45 89 f4 e9 04 ff ff ff e8 00 74 09 f8 44 89 f0 99 <f7> 7c</f7>		
			24 14 41 29 d6 45 89 f4 e9 ec fe ff ff e8 e8 73 09 f8 48 89		
			RSP: 0018:ffffc900041f7930 EFLAGS: 00010293		
			RAX: 0000000000017e67 RBX: 0000000000017e67 RCX: ffffffff8983314b		
			RDX: 0000000000000000 RSI: ffffffff898331b0 RDI: 0000000000000004		
			RBP: 00000000005d6000 R08: 0000000000000004 R09: 0000000000017e67		
			R10: 000000000003e80 R11: 0000000000000000 R12: 0000000000003e80		

0-1

1-2

2-3

4-5 5-6 6-7

7-8 8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R13: ffff888031d9b440 R14: 0000000000017e67 R15: 00000000002eb000		
			FS: 00007feb5d7f16c0(0000) GS:ffff8880b8700000(0000		
) knlGS:000000000000000000		
			CS: 0010 DS: 0000 ES: 0000 CR0: 000000080050033		
			CR2: 00007feb5d8adbb8 CR3: 0000000074e4c000 CR4: 0000000003526f0		
			DR0: 00000000000000000 DR1: 00000000000000000 DR2: 0000000000000000000		
			DR3: 00000000000000000 DR6: 00000000fffe0ff0 DR7: 00000000000000400		
			Call Trace:		
			<task></task>		
			tcp_cleanup_rbuf+0x3e7/ 0x4b0 net/ipv4/tcp.c:1493		
			mptcp_rcv_space_adjust net/mptcp/protocol.c:2085 [inline]		
			mptcp_recvmsg+0x2156/0x 2600		
			net/mptcp/protocol.c:2289		
			inet_recvmsg+0x469/0x6a0 net/ipv4/af_inet.c:885		
			sock_recvmsg_nosec net/socket.c:1051 [inline]		
			sock_recvmsg+0x1b2/0x25 0 net/socket.c:1073		
			sys_recvfrom+0x1a5/0x2 e0 net/socket.c:2265		
			do_sys_recvfrom net/socket.c:2283 [inline]		
CVSSv3 Scoring *stands for all v		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
			se_sys_recvfrom net/socket.c:2279 [inline]		
			x64_sys_recvfrom+0xe0/0 x1c0 net/socket.c:2279		
			do_syscall_x64 arch/x86/entry/common.c: 52 [inline]		
			do_syscall_64+0xcd/0x250 arch/x86/entry/common.c: 83		
			entry_SYSCALL_64_after_hw frame+0x77/0x7f		
			RIP: 0033:0x7feb5d857559		
			Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 51 18 00 00 90 48 89 f8 48		
			89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d		
			01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48		
			RSP: 002b:00007feb5d7f1208 EFLAGS: 00000246 ORIG_RAX: 00000000000002d		
			RAX: fffffffffffffffda RBX: 00007feb5d8e1318 RCX: 00007feb5d857559		
			RDX: 000000800000000e RSI: 0000000000000000 RDI: 00000000000000003		
			RBP: 00007feb5d8e1310 R08: 0000000000000000 R09: fffffff81000000		
			R10: 00000000000000000 R11: 0000000000000246 R12: 00007feb5d8e131c		

4-5 5-6 3-4

7-8 8-9

9-10

6-7

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R13: 00007feb5d8ae074 R14: 0000080000000e R15: 00000000fffffdef		
			and provided a nice reproducer.		
			The root cause is the current bad handling of racing disconnect.		
			After the blamed commit below, sk_wait_data() can return (with		
			error) with the underlying socket disconnected and a zero rcv_mss.		
			Catch the error and return without performing any additional		
			operations on the current socket.		
Affected Ver	sion(s): From (i	ncluding)	CVE ID : CVE-2024-53123 6.6.0 Up to (excluding) 6.6.63		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/0 b364cf5	
N/A	04-Dec-2024	7.8	vdpa: solidrun: Fix UB bug with devres	3b2020 4e92bac 7c6ebd1 ee7d3ec	O-LIN-LINU- 241224/1551
			In psnet_open_pf_bar() and snet_open_vf_bar() a string later passed to pcim_iomap_regions() is placed on the stack. Neither	62931, https:// git.kerne l.org/sta ble/c/5 bb287da 2d2d5b	
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
			pcim_iomap_regions() nor the functions it calls copy that string. Should the string later ever	b8f7376 e223b02 edb1699 8982e, https://	
			be used, this, consequently, causes	git.kerne l.org/sta ble/c/d	
			undefined behavior since the stack frame will by then have disappeared.	372dd0 9cfbf132 4f54cbff d81fcaf6	
			Fix the bug by allocating the strings on the heap through	cdf3e60 8e	
			devm_kasprintf().		
			CVE ID : CVE-2024-53126		
			In the Linux kernel, the following vulnerability has been resolved: drm/rockchip: vop: Fix a dereferenced before check	https:// git.kerne l.org/sta ble/c/1e 530597 29691ca 4d9051 18258b	
NULL Pointer	04-Dec-2024	5.5	The 'state' can't be NULL, we should check crtc_state.	9fbd17d 854174, https:// git.kerne l.org/sta	O-LIN-LINU-
Dereferenc e			Fix warning:	ble/c/6 56dbd1c 21c2c08	241224/1552
			drivers/gpu/drm/rockchip /rockchip_drm_vop.c:1096	8c70059 cdd43ec	
			vop_plane_atomic_async_ch eck() warn: variable dereferenced before check	83e7d54 ec4d, https://	
			'state' (see line 1077)	git.kerne l.org/sta	
			CVE ID : CVE-2024-53129	ble/c/ab 1c793f4 57f740a	

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				b7108cc 0b1340a 402dbf4 84d	
NULL Pointer Dereferenc e	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix null-ptr-deref in block_dirty_buffer tracepoint When using the "block:block_dirty_buffer" tracepoint, mark_buffer_dirty() may cause a NULL pointer dereference, or a general protection fault when KASAN is enabled. This happens because, since the tracepoint was added in mark_buffer_dirty(), it references the dev_t member bh->b_bdev- >bd_dev regardless of whether the buffer head has a pointer to a block_device structure. In the current implementation, nilfs_grab_buffer(), which grabs a buffer to read (or create) a block of metadata, including b- tree node blocks,	https:// git.kerne l.org/sta ble/c/2 026559a 6c4ce34 db117d 2db8f71 0fe2a94 20d5a, https:// git.kerne l.org/sta ble/c/7a f3309c7 a2ef268 31a6712 5b11c34 a7e01c1 b2a, https:// git.kerne l.org/sta ble/c/8 6b1903 1dbc79a bc378df ae357f6 ea33ebe b0c95	0-LIN-LINU- 241224/1553
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not set the block device, but instead does so only if the buffer is		
			not in the "uptodate" state for each of its caller block reading		
			functions. However, if the uptodate flag is set on a folio/page, and the		
			buffer heads are detached from it by try_to_free_buffers(), and new buffer		
			heads are then attached by create_empty_buffers(), the uptodate flag may		
			be restored to each buffer without the block device being set to		
			bh->b_bdev, and mark_buffer_dirty() may be called later in that state,		
			resulting in the bug mentioned above.		
			Fix this issue by making nilfs_grab_buffer() always set the block device		
			of the super block structure to the buffer head, regardless of the state		
			of the buffer's uptodate flag.		
			CVE ID : CVE-2024-53130	http://	
NULL Pointer Dereferenc e	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/0 85556bf 8c70e26	O-LIN-LINU- 241224/1554
CVSSv3 Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	29e02e7	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nilfs2: fix null-ptr-deref in block_touch_buffer tracepoint	9268dac 3016a08 b8bf, https://	
			Patch series "nilfs2: fix null- ptr-deref bugs on block tracepoints".	git.kerne l.org/sta ble/c/3 b2a4fd9 bbee77a	
			This series fixes null pointer dereference bugs that occur when using nilfs2 and two block-related tracepoints.	fdd3ed5 a05a0c0 2b6cde8 d3b9, https:// git.kerne l.org/sta	
			This patch (of 2):	ble/c/5 9b49ca6 7cca7b0 07a5afd	
			It has been reported that when using "block:block_touch_buffer"	3de0283 c800815 7665	
			tracepoint, touch_buffer() called from nilfs_get_folio_block() causes a		
			NULL pointer dereference, or a general protection fault when KASAN is enabled.		
			This happens because since		
			the tracepoint was added in touch_buffer(), it		
			references the dev_t member bh->b_bdev- >bd_dev regardless of whether the		

5-6 6-7 7-8

8-9

9-10

2-3

1-2

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer head has a pointer to a block_device structure. In the current		
			implementation, the block_device structure is set after the function		
			returns to the caller.		
			Here, touch_buffer() is used to mark the folio/page that owns the buffer		
			head as accessed, but the common search helper for folio/page used by the		
			caller function was optimized to mark the folio/page as accessed when it		
			was reimplemented a long time ago, eliminating the need to call		
			touch_buffer() here in the first place.		
			So this solves the issue by eliminating the touch_buffer() call itself.		
			CVE ID : CVE-2024-53131		
Affected Ver	sion(s): From (i	ncluding)	6.6.51 Up to (excluding) 6.6.63	I	
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/0 0bff717	
N/A	04-Dec-2024	5.5	Revert "mmc: dw_mmc: Fix IDMAC operation with pages bigger than 4K"	45bc358 3bd5ca5 9be91e0 ee1d27f 1944,	O-LIN-LINU- 241224/1555
	Scale 0-1	1-2 2	- 3 3-4 4-5 5-6	https://	20 040
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The commit 8396c793ffdf ("mmc: dw_mmc: Fix IDMAC operation with pages bigger than 4K") increased the max_req_size, even for 4K pages, causing various issues: - Panic booting the kernel/rootfs from an SD card on Rockchip RK3566 - Panic booting the kernel/rootfs from an SD card on StarFive JH7100 - "swiotlb buffer is full" and data corruption on StarFive JH7110 At this stage no fix have been found, so it's probably better to just revert the change. This reverts commit 8396c793ffdf28bb8aee7cfe 0891080f8cab7890.	git.kerne l.org/sta ble/c/1 635e407 a4a64d0 8a8517a c59ca14 ad4fc78 5e75, https:// git.kerne l.org/sta ble/c/5 6de724c 58c07a7 ca3aac0 27cfd2c cb184ed 9e4e	
Affected Ver	sion(s): From (i	ncluding)	6.6.60 Up to (excluding) 6.6.63	3	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	04-Dec-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: mm: revert "mm: shmem: fix data-race in shmem_getattr()"	https:// git.kerne l.org/sta ble/c/3 6b537e8 f302f67 0c7cf35 d88a3a2 94443e3 2d52, https:// git.kerne	O-LIN-LINU- 241224/1556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Revert d949d1d14fa2 ("mm: shmem: fix data-race in shmem_getattr()") as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over NFS.	l.org/sta ble/c/5 874c115 0e77296 565ad6e 495ef41 fbf8757 0d14,	
			As Hugh commented, "added just to silence a syzbot sanitizer splat: added where there has never been any practical problem". CVE ID : CVE-2024-53136	https:// git.kerne l.org/sta ble/c/6 4e67e86 94252c1 bf01b80 2ee911b e3fee62 c36b	
Affected Ver	sion(s): From (i	ncluding)	6.7 Up to (excluding) 6.11.10		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/0	
			sctp: fix possible UAF in sctp_v6_available()	5656a66 592759 242c740 636162	
Use After	04-Dec-2024	7.8	A lockdep report [1] with CONFIG_PROVE_RCU_LIST= y hints	91b727 4d11b2f, https:// git.kerne	O-LIN-LINU-
Free			that sctp_v6_available() is calling dev_get_by_index_rcu()	l.org/sta ble/c/ad 975697 211f4f2c	241224/1557
			and ipv6_chk_addr() without holding rcu.	4ce61c3 ba524fd 14d88ce	
			[1]	ab8, https://	
			=======	git.kerne l.org/sta ble/c/eb	

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
			WARNING: suspicious RCU usage 6.12.0-rc5-virtme #1216 Tainted: G W net/core/dev.c:876 RCU- list traversed in non-reader section!!	72e7fcc 83987d 5d5595 b43222f 23b295 d5de7f	
			other info that might help us debug this:		
			rcu_scheduler_active = 2, debug_locks = 1		
			1 lock held by sctp_hello/31495:		
			#0: ffff9f1ebbdb7418 (sk_lock-AF_INET6){+.+.}- {0:0}, at: sctp_bind (./arch/x86/include/asm/j ump_label.h:27 net/sctp/socket.c:315) sctp		
			stack backtrace: CPU: 7 UID: 0 PID: 31495 Comm: sctp_hello Tainted: G W 6.12.0-rc5- virtme #1216 Tainted: [W]=WARN		
			Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian- 1.16.3-2 04/01/2014		
			Call Trace:		
			<task></task>		
			dump_stack_lvl (lib/dump_stack.c:123)		

4-5 5-6 6-7

7-8 8-9

9-10

0-1

1-2

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIP	CID
			lockdep_rcu_suspicious (kernel/locking/lockdep.c:6 822)			
			dev_get_by_index_rcu (net/core/dev.c:876 (discriminator 7))			
			sctp_v6_available (net/sctp/ipv6.c:701) sctp			
			sctp_do_bind (net/sctp/socket.c:400 (discriminator 1)) sctp			
			sctp_bind (net/sctp/socket.c:320) sctp			
			inet6_bind_sk (net/ipv6/af_inet6.c:465)			
			? security_socket_bind (security/security.c:4581 (discriminator 1))			
			sys_bind (net/socket.c:1848 net/socket.c:1869)			
			? do_user_addr_fault (./include/linux/rcupdate.h :347			
			 ./include/linux/rcupdate.h: 880 ./include/linux/mm.h:729 arch/x86/mm/fault.c:1340) 			
			? do_user_addr_fault (./arch/x86/include/asm/p reempt.h:84 (discriminator 13)			
			 ./include/linux/rcupdate.h: 98 (discriminator 13) /include/linux/rcupdate.h; 			
			./include/linux/rcupdate.h:882 (discriminator 13)./include/linux/mm.h:729			
			(discriminator 13) arch/x86/mm/fault.c:1340			
			(discriminator 13))			
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
			x64_sys_bind (net/socket.c:1877 (discriminator 1) net/socket.c:1875 (discriminator 1) net/socket.c:1875 (discriminator 1)) do_syscall_64 (arch/x86/entry/common.c :52 (discriminator 1) arch/x86/entry/common.c: 83 (discriminator 1))		
			entry_SYSCALL_64_after_hw frame (arch/x86/entry/entry_64. S:130) RIP: 0033:0x7f59b934a1e7 Code: 44 00 00 48 8b 15 39 8c 0c 00 f7 d8 64 89 02 b8 ff ff ff ff eb bd 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 b8 31 00 00 00 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d 09 8c 0c 00 f7 d8 64 89 01 48		
			All code ======= 0: 44 00 00 add %r8b,(%rax) 3: 48 8b 15 39 8c 0c 00 mov 0xc8c39(%rip),%rdx # 0xc8c43 a: f7 d8 neg %eax c: 64 89 02 mov %eax,%fs:(%rdx)		

4-5 5-6 6-7

7-8 8-9

9-10

s for all versions

0-1

1-2

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f: b8 ff ff ff ff mov \$0xffffffff,%eax		
			14: eb bd jmp 0xffffffffffffd3		
			16: 66 2e 0f 1f 84 00 00 cs nopw		
			0x0(%rax,%rax,1)		
			1d: 00 00 00		
			20: 0f 1f 00 nopl (%rax)		
			23: b8 31 00 00 00 mov \$0x31,%eax		
			28: 0f 05 syscall		
			2a:* 48 3d 01 f0 ff ff		
			cmp \$0xffffffffffffff001,%rax < trapping		
			instruction		
			30: 73 01 jae 0x33		
			32: c3 ret		
			33: 48 8b 0d 09 8c 0c 00 mov		
			0xc8c09(%rip),%rcx # 0xc8c43		
			3a: f7 d8 neg %eax		
			3c: 64 89 01 mov		
			%eax,%fs:(%rcx)		
			3f: 48 rex.W		
			Code starting with the faulting instruction		
			=======================================		
			=		

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
			0: 48 3d 01 f0 ff ff cmp \$0xffffffffffffff001,%rax		
			6: 73 01 jae 0x9		
			8: c3 ret		
			9: 48 8b 0d 09 8c 0c 00		
			mov 0xc8c09(%rip),%rcx # 0xc8c19		
			10: f7 d8 neg %eax		
			12: 64 89 01 mov		
			%eax,%fs:(%rcx)		
			15: 48 rex.W RSP:		
			002b:00007ffe2d0ad398 EFLAGS: 00000202 ORIG_RAX: 000000000000031		
			RAX: fffffffffffffffda RBX: 00007ffe2d0ad3d0 RCX: 00007f59b934a1e7		
			RDX: 0000000000000001c RSI: 00007ffe2d0ad3d0 RDI: 00000000000000005		
			RBP: 00000000000000005 R08: 19999999999999999 R09: 00000000000000000		
			R10: 00007f59b9253298 R11: 000000000000		
			truncated		
			CVE ID : CVE-2024-53139		
Out-of- bounds Read	02-Dec-2024	7.1	In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/0a 326fbc8f	O-LIN-LINU- 241224/1558

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drm/amd/display: Adjust VSDB parser for replay feature	72a3200 51f2732 8d4d4e7 abdfe68	
			At some point, the IEEE ID identification for the replay check in the AMD EDID was added. However, this check causes the following out-of-bounds issues when using KASAN:	d7, https:// git.kerne l.org/sta ble/c/1 6dd282 5c23530 f2259fc6 71960a3 a65d2af	
			 [27.804016] BUG: KASAN: slab-out-of-bounds in amdgpu_dm_update_freesy nc_caps+0xefa/0x17a0 [amdgpu] [27.804788] Read of size 1 at addr ffff8881647fdb00 by task systemd-udevd/383 	69bd, https:// git.kerne l.org/sta ble/c/8 db8670 61f4c76 505ad62 422b65 d666b4 528921	
			 [27.821207] Memory state around the buggy address:	7	
			[27.821215] ffff8881647fda00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
			[27.821224] ffff8881647fda80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
			[27.821234] >ffff8881647fdb00: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc		
CVSSv3 Scoring *stands for all v		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
			[27.821243] ^ [27.821250] ffff8881647fdb80: fc fc fc fc fc fc fc fc fc fc fc fc fc fc		
			[27.821259] ffff8881647fdc00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
			[27.821268] ====================================		
			===		
			This is caused because the ID extraction happens outside of the range of		
			the edid lenght. This commit addresses this issue by considering the		
			amd_vsdb_block size.		
			(cherry picked from commit b7e381b1ccd5e778e3d9c4 4c669ad38439a861d8)		
			CVE ID : CVE-2024-53108		
	04-Dec-2024 6	4-Dec-2024 6.5	In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta	
N/A			KVM: VMX: Bury Intel PT virtualization (guest/host mode) behind CONFIG_BROKEN	ble/c/aa 0d42cac f093a6fc ca872ed c954f6f8 12926a1	O-LIN-LINU- 241224/1559
			Hide KVM's pt_mode module param behind CONFIG_BROKEN, i.e. disable support	7, https:// git.kerne l.org/sta ble/c/b	
CVSSv3 Scoring stands for all v		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for virtualizing Intel PT via guest/host mode unless BROKEN=y. There are	91bb0ce 5cd7005 b376eac	
			myriad bugs in the implementation, some of which are fatal to the guest,	690ec66 4c1b563 72ec, https://	
			and others which put the stability and health of the host at risk.	git.kerne l.org/sta ble/c/d 28b059e	
			For guest fatalities, the most glaring issue is that KVM fails to ensure	e4779b5 102c5da 6e92976 252051	
			tracing is disabled, and *stays* disabled prior to VM-Enter, which is	0e406	
			necessary as hardware disallows loading (the guest's) RTIT_CTL if tracing		
			is enabled (enforced via a VMX consistency check). Per the SDM:		
			If the logical processor is operating with Intel PT enabled (if		
			IA32_RTIT_CTL.TraceEn = 1) at the time of VM entry, the "load		
			IA32_RTIT_CTL" VM-entry control must be 0.		
			On the host side, KVM doesn't validate the guest CPUID configuration		
			provided by userspace, and even worse, uses the guest configuration to		

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
			decide what MSRs to save/load at VM-Enter and VM-Exit. E.g. configuring		
			guest CPUID to enumerate more address ranges than are supported in hardware		
			will result in KVM trying to passthrough, save, and load non-existent MSRs,		
			which generates a variety of WARNs, ToPA ERRORs in the host, a potential		
			deadlock, etc.		
			CVE ID : CVE-2024-53135		
Integer Overflow or Wraparoun d	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fs/proc/task_mmu: prevent integer overflow in pagemap_scan_get_args() The "arg->vec_len" variable is a u64 that comes from the user at the start of the function. The "arg- >vec_len * sizeof(struct page_region))" multiplication can lead to integer wrapping. Use size_mul() to avoid that. Also the size_add/mul() functions work on unsigned long so for 32bit	https:// git.kerne l.org/sta ble/c/6 69b0cb8 1e4e4e7 8cff77a5 b367c7f 70c0c6c 05e, https:// git.kerne l.org/sta ble/c/ad ee03f89 03c58a6 a559f21 388a430 211fac8 ce9	O-LIN-LINU- 241224/1560

CVSSv3 Scoring Scale

0-1

1-2

2-3

5-6 6-7 8-9

9-10

7-8

*stands for all versions

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			systems we need to ensure that "arg->vec_len" fits in an unsigned long.		
			CVE ID : CVE-2024-53107		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta	
		ec-2024 5.5	nommu: pass NULL argument to vma_iter_prealloc()	ble/c/2 47d720 b2c5d22 f728143 7fd6054 a138256	O-LIN-LINU- 241224/1561
			When deleting a vma entry from a maple tree, it has to pass NULL to	986ba, https:// git.kerne	
N/A	02-Dec-2024		vma_iter_prealloc() in order to calculate internal state of the tree, but	l.org/sta ble/c/8 bbf0ab6 31cdf1d ade6745 f137cff9 8751e6c	
,			it passed a wrong argument. As a result, nommu kernels crashed upon		
			accessing a vma iterator, such as acct_collect() reading the size of vma	ed7, https:// git.kerne	
			entries after do_munmap().	l.org/sta ble/c/ac eaf33b7	
			This commit fixes this issue by passing a right argument to the	666b72 dfb86e0 aa977be	
			preallocation call.	81e3bcb	
			CVE ID : CVE-2024-53109	c727	
N/A 02	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/0a	O-LIN-LINU- 241224/1562
	02 000 2024		vp_vdpa: fix id_table array not null terminated error	886489 d27459 6ad1a80 789d3a7	
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
			Allocate one extra virtio_device_id as null terminator, otherwise vdpa_mgmtdev_get_classes() may iterate multiple times and visit undefined memory. CVE ID : CVE-2024-53110	735032 10a615, https:// git.kerne l.org/sta ble/c/4e 39ecadf 1d2a081 871396 19f1f31 4b64ba7 d947, https:// git.kerne l.org/sta ble/c/8 70d68fe 17b5d9 032049 dcad98b 5781a34 4a8657	
Integer Overflow or Wraparoun d	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/mremap: fix address wraparound in move_page_tables() On 32-bit platforms, it is possible for the expression `len + old_addr < old_end` to be false-positive if `len + old_addr` wraps around. `old_addr` is the cursor in the old range up to which page table entries	https:// git.kerne l.org/sta ble/c/9 09543dc 279a911 22fb08e 4653a72 b82f0ad 28f4, https:// git.kerne l.org/sta ble/c/a4 a282daf 1a190f0 3790bf1 63458ea 3c8d28d 217	O-LIN-LINU- 241224/1563

4-5 3-4

5-6

6-7

9-10

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID			Pa	atch	NCIIP	CID
			have been n operation su `old_addr` is	ucceeded	l,				
			-	the old region, and adding `len` to it can wrap.					
			The overflow mremap() to believe that	o mistak	enly	1			
			copied; the o that mrema doesn't mov	p() bails		t			
			PTEs back b VMA is unm anonymous	apped, c	ausing				
			region to be basically if u to mremap(iserspac					
			private-ano hits this bug return an er	g, mrema		l			
			the private- contents ap been zeroed	pear to h	-				
			The idea of t `old_end - le start						
			address, and check that w it easier to r	vay also	•				
			fix the check the compari	-					
			(An alternat to refactor t introducing	his funct					
			"orig_old_sta such.)	art" vari	able or				
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	NCIIP	C ID
			Tested in a VM with a 32-bit X86 kernel; without the			
			patch:			
			user@horn:~/big_mremap\$ cat test.c			
			#define _GNU_SOURCE			
			#include <stdlib.h></stdlib.h>			
			<pre>#include <stdio.h></stdio.h></pre>			
			<pre>#include <err.h></err.h></pre>			
			<pre>#include <sys mman.h=""></sys></pre>			
			#define ADDR1 ((void*)0x60000000)			
			#define ADDR2			
			((void*)0x10000000)			
			#define SIZE 0x50000000uL			
			ond of of of of our			
			int main(void) {			
			unsigned char *p1 =			
			mmap(ADDR1, SIZE, PROT_READ PROT_WRITE,			
			MAP_ANONYMOUS MAP_PR			
			IVATE MAP_FIXED_NOREPL ACE, -1, 0);			
			if $(p1 == MAP_FAILED)$			
			err(1, "mmap 1");			
			unsigned char *p2 =			
			mmap(ADDR2, SIZE, PROT_NONE,			
			1 NO 1_NO 11L,			
			MAP_ANONYMOUS MAP_PR			
CVSSv3 Scoring	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5-6 (6-7 7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IVATE MAP_FIXED_NOREPL		
			ACE, -1, 0);		
			if (p2 == MAP_FAILED)		
			err(1, "mmap 2");		
			*p1 = 0x41;		
			printf("first char is 0x%02hhx\n", *p1);		
			unsigned char *p3 = mremap(p1, SIZE, SIZE,		
			MREMAP_MAYMOVE MRE MAP_FIXED, p2);		
			if (p3 == MAP_FAILED) {		
			printf("mremap() failed; first char is 0x%02hhx\n", *p1);		
			} else {		
			printf("mremap() succeeded; first char is 0x%02hhx\n", *p3);		
			}		
			}		
			user@horn:~/big_mremap\$ gcc -static -o test test.c		
			user@horn:~/big_mremap\$ setarch -R ./test		
			first char is 0x41		
			mremap() failed; first char is 0x00		

			With the patch:		

			user@horn:~/big_mremap\$ setarch -R ./test		

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			first char is 0x41 mremap() succeeded; first char is 0x41 CVE ID : CVE-2024-53111		
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ocfs2: uncache inode which has failed entering the group Syzbot has reported the following BUG: kernel BUG at fs/ocfs2/uptodate.c:509! Call Trace: <task> ?die_body+0x5f/0xb0 ? die+0x9e/0xc0 ? do_trap+0x15a/0x3a0 ? ocfs2_set_new_buffer_uptod ate+0x145/0x160 ? do_error_trap+0x1dc/0x2c 0 ? ocfs2_set_new_buffer_uptod ate+0x145/0x160 ? jocfs2_set_new_buffer_uptod ate+0x145/0x160 ?</task>	https:// git.kerne l.org/sta ble/c/6 20d225 98110b 0d0cb97 a3fcca65 fc473ea 86e73, https:// git.kerne l.org/sta ble/c/7 37f3413 7844d6 572ab7d 473c998 c7f977ff 30eb, https:// git.kerne l.org/sta ble/c/8 43dfc80 4af4b33 8ead423 31dd58 081b42 8ecdf8	O-LIN-LINU- 241224/1564

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
			? handle_invalid_op+0x34/0x 40		
			? ocfs2_set_new_buffer_uptod ate+0x145/0x160		
			? exc_invalid_op+0x38/0x50 ?		
			asm_exc_invalid_op+0x1a/0 x20		
			? ocfs2_set_new_buffer_uptod ate+0x2e/0x160		
			? ocfs2_set_new_buffer_uptod ate+0x144/0x160		
			? ocfs2_set_new_buffer_uptod ate+0x145/0x160		
			ocfs2_group_add+0x39f/0x 15a0		
			? pfx_ocfs2_group_add+0x1 0/0x10		
			? pfx_lock_acquire+0x10/0x 10		
			? mnt_get_write_access+0x68 /0x2b0		
			? pfx_lock_release+0x10/0x 10		
			? rcu_read_lock_any_held+0x b7/0x160		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? pfx_rcu_read_lock_any_hel d+0x10/0x10		
			? smack_log+0x123/0x540		
			? mnt_get_write_access+0x68 /0x2b0		
			?		
			mnt_get_write_access+0x68 /0x2b0		
			?		
			mnt_get_write_access+0x22 6/0x2b0		
			ocfs2_ioctl+0x65e/0x7d0		
			? pfx_ocfs2_ioctl+0x10/0x1 0		
			? smack_file_ioctl+0x29e/0x3 a0		
			?		
			pfx_smack_file_ioctl+0x10 /0x10		
			? lockdep_hardirqs_on_prepa re+0x43d/0x780		
			?		
			pfx_lockdep_hardirqs_on_ prepare+0x10/0x10		
			? pfx_ocfs2_ioctl+0x10/0x1		
			0		
			se_sys_ioctl+0xfb/0x170 do_syscall_64+0xf3/0x230		
			entry_SYSCALL_64_after_hw frame+0x77/0x7f		

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
vveakness		CVSSV3	<pre>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>		
NULL Pointer Dereferenc e	02-Dec-2024 Scale 0-1	5.5	CVE ID : CVE-2024-53112 In the Linux kernel, the following vulnerability has been resolved: mm: fix NULL pointer dereference in alloc_pages_bulk_noprof We triggered a NULL pointer dereference for ac.preferred_zoneref->zone in alloc_pages_bulk_noprof() when the task is migrated between cpusets.	https:// git.kerne l.org/sta ble/c/3 150237 4627ba9 ec3e710 dbd0bb 00457cc 6d2c19, https:// git.kerne l.org/sta ble/c/6a ddb2d9 501ec86 6d7b3a3	0-LIN-LINU- 241224/1565

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When cpuset is enabled, in prepare_alloc_pages(), ac- >nodemask may be ¤t->mems_allowed. when first_zones_zonelist() is called to find	b4e6653 07c437e 9be2, https:// git.kerne l.org/sta ble/c/8c e41b0f9	
			preferred_zoneref, the ac- >nodemask may be modified concurrently if the	d77cca0 74df25a fd39b86	
			task is migrated between different cpusets. Assuming we have 2 NUMA Node,	e2ee3aa 68e	
			when traversing Node1 in ac->zonelist, the nodemask is 2, and when		
			traversing Node2 in ac- >zonelist, the nodemask is 1. As a result, the		
			ac->preferred_zoneref points to NULL zone.		
			In alloc_pages_bulk_noprof(), for_each_zone_zonelist_nod emask() finds a		
			allowable zone and calls zonelist_node_idx(ac.prefer red_zoneref), leading		
			to NULL pointer dereference.		
			alloc_pages_noprof() fixes this issue by checking NULL pointer in commit		
			ea57485af8f4 ("mm, page_alloc: fix check for NULL preferred_zone") and		

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
			commit df76cee6bbeb ("mm, page_alloc: remove redundant checks from alloc fastpath").		
			To fix it, check NULL pointer for preferred_zoneref->zone. CVE ID : CVE-2024-53113		
Missing Release of Memory after Effective Lifetime	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: virtio/vsock: Improve MSG_ZEROCOPY error handling Add a missing kfree_skb() to prevent memory leaks. CVE ID : CVE-2024-53117	https:// git.kerne l.org/sta ble/c/5 0061d7 319e211 65d04e3 024354c 1b43b6 137821, https:// git.kerne l.org/sta ble/c/6 0cf6206 a1f5135 12f5d73 fa4d3db bcad2e7 dcd6	O-LIN-LINU- 241224/1566
Missing Release of Memory after Effective Lifetime	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: vsock: Fix sk_error_queue memory leak Kernel queues MSG_ZEROCOPY completion	https:// git.kerne l.org/sta ble/c/be a4779a4 5f49275 b1e1b1b d9de03c d37272 44d8, https:// git.kerne	O-LIN-LINU- 241224/1567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			notifications on the error queue. Where they remain, until explicitly recv()ed. To prevent memory leaks, clean up the queue when the socket is destroyed.	l.org/sta ble/c/fb f7085b3 ad1c7cc 067783 4c90f98 5f1b4f7 7a33	
			unreferenced object 0xffff8881028beb00 (size 224):		
			comm "vsock_test", pid 1218, jiffies 4294694897		
			hex dump (first 32 bytes):		
			90 b0 21 17 81 88 ff ff 90 b0 21 17 81 88 ff ff!!		
			00 00 00 00 00 00 00 00 00 00 b0 21 17 81 88 ff ff 		
			backtrace (crc 6c7031ca):		
			[<ffffffff81418ef7>] kmem_cache_alloc_node_no prof+0x2f7/0x370</ffffffff81418ef7>		
			[<ffffffff81d35882>] alloc_skb+0x132/0x180</ffffffff81d35882>		
			[<ffffffff81d2d32b>] sock_omalloc+0x4b/0x80</ffffffff81d2d32b>		
			[<ffffffff81d3a8ae>] msg_zerocopy_realloc+0x9e /0x240</ffffffff81d3a8ae>		
			[<fffffffff81fe5cb2>] virtio_transport_send_pkt_i nfo+0x412/0x4c0</fffffffff81fe5cb2>		
			[<ffffffff81fe6183>] virtio_transport_stream_en queue+0x43/0x50</ffffffff81fe6183>		

0-1

1-2

2-3

5-6 6-7 7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[<fffffff81fe0813>] vsock_connectible_sendmsg +0x373/0x450 [<fffffff81d233d5>]</fffffff81d233d5></fffffff81fe0813>		
			sys_sendmsg+0x365/0x 3a0		
			[<ffffffff81d246f4>] sys_sendmsg+0x84/0xd0</ffffffff81d246f4>		
			[<ffffffff81d26f47>] sys_sendmsg+0x47/0x80</ffffffff81d26f47>		
			[<ffffffff820d3df3>] do_syscall_64+0x93/0x180</ffffffff820d3df3>		
			[<ffffffff8220012b>] entry_SYSCALL_64_after_hw frame+0x76/0x7e</ffffffff8220012b>		
			CVE ID : CVE-2024-53118		
	U U		In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/2	
			virtio/vsock: Fix accept_queue memory leak	415345 042245 de7601d cc6eafdb	
Missing Release of			As the final stages of socket destruction may be delayed, it is possible	e3a3dcc 9e379, https:// git.kerne	
Memory after Effective Lifetime	02-Dec-2024	02-Dec-2024 5.5	that virtio_transport_recv_listen () will be called after the accept_queue	l.org/sta ble/c/8 97617a4 13e0bf1	O-LIN-LINU- 241224/1568
			has been flushed, but before the SOCK_DONE flag has been set. As a result,	c6380e3 b34b2f2 8f45050 8549,	
			sockets enqueued after the flush would remain unremoved, leading to a	https:// git.kerne l.org/sta	
			memory leak.	ble/c/9 46c7600 fa2207c	
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
			vsock_release	c8d3fbc	
			vsock_release	86a518e c56f98a	
			lock	5813	
			virtio_transport_release		
			virtio_transport_close		
			schedule_delayed_work(clo se_work)		
			sk_shutdown = SHUTDOWN_MASK		
			(!) flush accept_queue		
			release		
			virtio_transport_recv_pkt		
			vsock_find_bound_socket		
			lock		
			if flag(SOCK_DONE) return		
			virtio_transport_recv_listen child		
			= vsock_create_connected		
			(!) vsock_enqueue_accept(child)		
			release		
			close_work		
			lock		
			virtio_transport_do_close		
			set_flag(SOCK_DONE)		
			virtio_transport_remove_so ck		
			vsock_remove_sock		

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vsock_remove_bound		
			release		
			Introduce a sk_shutdown		
			check to disallow vsock_enqueue_accept()		
			during		
			socket destruction.		
			unreferenced object		
			0xffff888109e3f800 (size		
			2040):		
			comm "kworker/5:2", pid 371, jiffies 4294940105		
			hex dump (first 32 bytes):		
			00 00 00 00 00 00 00 00		
			00 00 00 00 00 00 00 00		
			28 00 0b 40 00 00 00 00		
			00 00 00 00 00 00 00 00 00		
			(@		
			backtrace (crc 9e5f4e84):		
			[<fffffff81418ff1>]</fffffff81418ff1>		
			kmem_cache_alloc_noprof+ 0x2c1/0x360		
			[<ffffffff81d27aa0>]</ffffffff81d27aa0>		
			sk_prot_alloc+0x30/0x120		
			[<ffffffff81d2b54c>] sk_alloc+0x2c/0x4b0</ffffffff81d2b54c>		
			[<ffffffff81fe049a>]</ffffffff81fe049a>		
			vsock_create.constprop.0+		
			0x2a/0x310		
			[<ffffffff81fe6d6c>] virtio_transport_recv_pkt+0</ffffffff81fe6d6c>		
			x4dc/0x9a0		
			[<ffffffff81fe745d>]</ffffffff81fe745d>		
			vsock_loopback_work+0xfd		
			/0x140		
CVSSv3 Scoring		1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

[<fffffff810fc6ac>] process_one_work+0x20c/0 x570 [<fffffff810fce3f>] worker_thread+0x1bf/0x3a 0 [<fffffff811070dd>] kthread+0xdd/0x110 [<fffffff81044fdd>] ret_from_fork+0x2d/0x50 [<fffffff8100785a>] ret_from_fork_asm+0x1a/0 x30 CVE ID : CVE-2024-53119 In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: CT: Fix null-ptr- deref in add rule err flow JIn error flow of</fffffff8100785a></fffffff81044fdd></fffffff811070dd></fffffff810fce3f></fffffff810fc6ac>	CIIPC ID
worker_thread+0x1bf/0x3a 0 [<ffffffff811070dd>] kthread+0xdd/0x110 [<fffffff81044fdd>] ret_from_fork+0x2d/0x50 [<fffffff8100785a>] ret_from_fork_asm+0x1a/0 x30 CVE ID : CVE-2024-53119 In the Linux kernel, the following vulnerability has been resolved: In the Linux kernel, the following vulnerability has been resolved: In et/mlx5e: CT: Fix null-ptr- deref in add rule err flow bd2f006 798557 d2a3210</fffffff8100785a></fffffff81044fdd></ffffffff811070dd>	
kthread+0xdd/0x110[<ffffffff81044fdd>]ret_from_fork+0x2d/0x50[<ffffffff8100785a>]ret_from_fork_asm+0x1a/0x30CVE ID : CVE-2024-53119In the Linux kernel, the following vulnerability has been resolved:lin the Linux kernel, the following vulnerability has ble/c/0https:// git.kerne l.org/sta ble/c/0net/mlx5e: CT: Fix null-ptr- deref in add rule err flowhttps:// d2a3210</ffffffff8100785a></ffffffff81044fdd>	
ret_from_fork+0x2d/0x50 [<ffffffff8100785a>] ret_from_fork_asm+0x1a/0 x30 CVE ID : CVE-2024-53119 In the Linux kernel, the following vulnerability has been resolved: https:// git.kerne l.org/sta ble/c/0 6dc488a 593020 bd2f006 798557 d2a3210</ffffffff8100785a>	
ret_from_fork_asm+0x1a/0 x30ret_from_fork_asm+0x1a/0 x30CVE ID : CVE-2024-53119https:// git.kerne l.org/sta ble/c/0 6dc488a ble/c/0 6dc488a 593020 bd2f006 798557 d2a3210	
Image: constraint of the state of the sta	
following vulnerability has been resolved: het/mlx5e: CT: Fix null-ptr- deref in add rule err flow bd2f006 798557 d2a3210	
net/mlx5e: CT: Fix null-ptr- deref in add rule err flow 798557 d2a3210	
In error flow of	
mlx5_tc_ct_entry_add_rule() , in case ct_rule_add() git.kerne	
NULL Pointer Dereferenc02-Dec-2024callback returns error, solutionl.org/sta02-Dec-20245.5callback returns error, uninitiated. Fix it toble/c/0c0-LIN 2412	0-LIN-LINU- 241224/1569
e use attr which has the 696cfed needed pointer value. ba35041 1dca736 361ef9a	
Kernel log: 0f,	
BUG: kernel NULL pointer https:// dereference, address: git.kerne 00000000000110 l.org/sta	
RIP: 030f8bd 0010:mlx5_tc_ct_entry_add_ 7902e9e rule+0x2b1/0x2f0 276a0ed [mlx5_core] c09bf11	
CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-5	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				979e4e2	
			Call Trace:	bc2e	
			<task></task>		
			?_die+0x20/0x70		
			?		
			page_fault_oops+0x150/0x 3e0		
			?		
			exc_page_fault+0x74/0x140		
			?		
			asm_exc_page_fault+0x22/0 x30		
			?		
			mlx5_tc_ct_entry_add_rule+ 0x2b1/0x2f0 [mlx5_core]		
			?		
			mlx5_tc_ct_entry_add_rule+ 0x1d5/0x2f0 [mlx5_core]		
			mlx5_tc_ct_block_flow_offlo ad+0xc6a/0xf90 [mlx5_core]		
			?		
			nf_flow_offload_tuple+0xd8 /0x190 [nf_flow_table]		
			nf_flow_offload_tuple+0xd8 /0x190 [nf_flow_table]		
			flow_offload_work_handler+ 0x142/0x320 [nf_flow_table]		
			? finish_task_switch.isra.0+0x 15b/0x2b0		
			process_one_work+0x16c/0 x320		

0-1

1-2

2-3

3-4 4-5

5-6

6-7

7-8

8-9

			worker_thread+0x28c/0x3a		
			0 ? pfx_worker_thread+0x10/ 0x10 kthread+0xb8/0xf0 ? pfx_kthread+0x10/0x10 ret_from_fork+0x2d/0x50 ? pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0 x30 		
			CVE ID : CVE-2024-53120		
Concurrent Execution using Shared Resource with 02 Improper Synchroniz ation ('Race Condition')	2-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: fs, lock FTE when checking if active The referenced commits introduced a two-step process for deleting FTEs: - Lock the FTE, delete it from hardware, set the hardware deletion function to NULL and unlock the FTE. - Lock the parent flow group, delete the software copy of the FTE, and remove it from the xarray.	https:// git.kerne l.org/sta ble/c/0 94d1a21 21cee1e 85ab07d 74388f9 4809dcf b5b9, https:// git.kerne l.org/sta ble/c/9 33ef0d1 7f012b6 53e9e60 06e3f50 c8d0238 b5ed, https:// git.kerne l.org/sta ble/c/9c	O-LIN-LINU- 241224/1570
CVSSv3 Scoring Sca	ale 0-1	1-2 2	<mark>-3 3-4 4-5 5-6</mark>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			However, this approach encounters a race condition if a rule with the same match value is added simultaneously. In this scenario, fs_core may set the	a314419 930f913 5727e39 d77e662 62d5f7b ef6	
			hardware deletion function to NULL prematurely, causing a panic during		
			subsequent rule deletions.		
			To prevent this, ensure the active flag of the FTE is checked under a lock, which will prevent the fs_core layer from attaching		
			a new steering rule to		
			an FTE that is in the process of deletion.		
			[438.967589] MOSHE: 2496 mlx5_del_flow_rules del_hw_func		
			[438.968205][cut here]		
			[438.968654] refcount_t: decrement hit 0; leaking memory.		
			[438.969249] WARNING: CPU: 0 PID: 8957 at lib/refcount.c:31 refcount_warn_saturate+0xf b/0x110		
			[438.970054] Modules linked in: act_mirred cls_flower act_gact sch_ingress openvswitch		

0-1

1-2

2-3

Page **742** of **1137**

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
weakiless			nsh mlx5_vdpa vringh vhost_iotlb vdpa mlx5_ib mlx5_core xt_conntrack xt_MASQUERADE nf_conntrack_netlink nfnetlink xt_addrtype iptable_nat nf_nat br_netfilter rpcsec_gss_krb5 auth_rpcgss oid_registry overlay rpcrdma rdma_ucm ib_iser libiscsi scsi_transport_iscsi ib_umad rdma_cm ib_ipoib iw_cm ib_cm ib_uverbs ib_core zram zsmalloc fuse [last unloaded: cls_flower]	Fatch	
			[438.973288] CPU: 0 UID: 0 PID: 8957 Comm: tc Not tainted 6.12.0-rc1+ #8 [438.973888] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0- gf21b5a4aeb02- prebuilt.qemu.org 04/01/2014		
			[438.974874] RIP: 0010:refcount_warn_satura te+0xfb/0x110		
			[438.975363] Code: 40 66 3b 82 c6 05 16 e9 4d 01 01 e8 1f 7c a0 ff 0f 0b c3 cc cc cc cc 48 c7 c7 10 66 3b 82 c6 05 fd e8 4d 01 01 e8 05 7c a0 ff <0f> 0b c3 cc cc cc cc 66 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 90		
			[438.976947] RSP: 0018:ffff888124a53610 EFLAGS: 00010286		
			[438.977446] RAX: 0000000000000000 RBX:		
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
			ffff888119d56de0 RCX: 0000000000000000		
			[438.978090] RDX: ffff88852c828700 RSI: ffff88852c81b3c0 RDI: ffff88852c81b3c0		
			[438.978721] RBP: ffff888120fa0e88 R08: 0000000000000000 R09: ffff888124a534b0		
			[438.979353] R10: 0000000000000001 R11: 0000000000000001 R12: ffff888119d56de0		
			[438.979979] R13: ffff888120fa0ec0 R14: ffff888120fa0ee8 R15: ffff888119d56de0		
			[438.980607] FS: 00007fe6dcc0f800(0000) GS:ffff88852c800000(0000) knlGS:00000000000000000		
			[438.983984] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033		
			[438.984544] CR2: 00000000004275e0 CR3: 0000000186982001 CR4: 000000000372eb0		
			[438.985205] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 00000000000000000		
			[438.985842] DR3: 0000000000000000 DR6: 000000000fffe0ff0 DR7: 00000000000000400		
			[438.986507] Call Trace:		
			[438.986799] <task></task>		

3-4 4-5 5-6

7-8 8-9 9-10

6-7

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<pre>[438.987070] ?warn+0x7d/0x110 [438.987426] ? refcount_warn_saturate+0xf b/0x110</pre>		
			[438.987877] ? report_bug+0x17d/0x190		
			[438.988261] ? prb_read_valid+0x17/0x20		
			[438.988659] ? handle_bug+0x53/0x90		
			[438.989054] ? exc_invalid_op+0x14/0x70		
			[438.989458] ? asm_exc_invalid_op+0x16/0 x20		
			[438.989883] ? refcount_warn_saturate+0xf b/0x110		
			[438.990348] mlx5_del_flow_rules+0x2f7/ 0x340 [mlx5_core]		
			[438.990932] mlx5_eswitch_del_rule+0x 49/0x170 [mlx5_core]		
			[438.991519] ? mlx5_lag_is_sriov+0x3c/0x5 0 [mlx5_core]		
			[438.992054] ? xas_load+0x9/0xb0		
			[438.992407] mlx5e_tc_rule_unoffload+0x 45/0xe0 [mlx5_core]		
			[438.993037] mlx5e_tc_del_fdb_flow+0x2 a6/0x2e0 [mlx5_core]		
			[438.993623] mlx5e_flow_put+0x29/0x60 [mlx5_core]		
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5 5-6 0	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[438.994161] mlx5e_delete_flower+0x261 /0x390 [mlx5_core]		
			[438.994728] tc_setup_cb_destroy+0xb9/ 0x190		
			[438.995150] fl_hw_destroy_filter+0x94/ 0xc0 [cls_flower]		
			[438.995650] fl_change+0x11a4/0x13c0 [cls_flower]		
			[438.996105] tc_new_tfilter+0x347/0xbc0		
			[438.996503] ?		
			truncated		
			CVE ID : CVE-2024-53121		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/2	
Concurrent Execution using			mptcp: cope racing subflow creation in mptcp_rcv_space_adjust	499585 1d58c4a 205ad0f fa7b2f2 1e479a9	
Shared Resource with	02-Dec-2024	5.5	Additional active subflows - i.e. created by the in kernel path	c8527, https:// git.kerne l.org/sta	O-LIN-LINU- 241224/1571
Improper Synchroniz ation ('Race			manager - are included into the subflow list before starting the	ble/c/aa d6412c6 3baa39d	
Condition')			3whs.	d813e81	
				f16a14d 976b3de	
			A racing recvmsg() spooling	2e8,	
			data received on an already established	https://	
			subflow would	git.kerne l.org/sta	
			unconditionally call	ble/c/ce	

0-1

1-2

2-3

Page **746** of **1137**

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<pre>tcp_cleanup_rbuf() on all the current subflows, potentially hitting a divide by zero error on the newly created ones. Explicitly check that the subflow is in a suitable state before invoking tcp_cleanup_rbuf(). CVE ID : CVE-2024-53122</pre>	7356ae3 5943cc6 494cc69 2e62d51 a734062 b7d	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mptcp: error out earlier on disconnect Eric reported a division by zero splat in the MPTCP protocol: Oops: divide error: 0000 [#1] PREEMPT SMP KASAN PTI CPU: 1 UID: 0 PID: 6094 Comm: syz-executor317 Not tainted 6.12.0-rc5-syzkaller-00291- g05b92660cdfe #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/13/2024	https:// git.kerne l.org/sta ble/c/5 813022 98524e9 d77c4c4 4ff5156 a6cd112 227ae, https:// git.kerne l.org/sta ble/c/9 55388e1 d5d222c 4101c59 6b536d 41b91a8 b212e, https:// git.kerne l.org/sta ble/c/a6 6805c9b 22caf4e 42af7a6 16f6c6b	O-LIN-LINU- 241224/1572

0-1

1-2

2-3 3-4 4-5

Page 747 of 1137

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RIP: 0010:tcp_select_window+ 0x5b4/0x1310 net/ipv4/tcp_output.c:3163	83c90d1 010	
			Code: f6 44 01 e3 89 df e8 9b 75 09 f8 44 39 f3 0f 8d 11 ff ff ff e8		
			0d 74 09 f8 45 89 f4 e9 04 ff ff ff e8 00 74 09 f8 44 89 f0 99 <f7> 7c</f7>		
			24 14 41 29 d6 45 89 f4 e9 ec fe ff ff e8 e8 73 09 f8 48 89		
			RSP: 0018:ffffc900041f7930 EFLAGS: 00010293		
			RAX: 0000000000017e67 RBX: 0000000000017e67 RCX: ffffffff8983314b		
			RDX: 0000000000000000 RSI: ffffffff898331b0 RDI: 0000000000000004		
			RBP: 00000000005d6000 R08: 0000000000000004 R09: 0000000000017e67		
			R10: 000000000003e80 R11: 0000000000000000 R12: 000000000003e80		
			R13: ffff888031d9b440 R14: 000000000017e67 R15: 0000000002eb000		
			FS: 00007feb5d7f16c0(0000) GS:ffff8880b8700000(0000		
) knlGS:000000000000000000		
			CS: 0010 DS: 0000 ES: 0000 CR0: 000000080050033		

4-5 5-6 6-7

8-9

9-10

7-8

1-2

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CR2: 00007feb5d8adbb8 CR3: 0000000074e4c000 CR4: 0000000003526f0		
			DR0: 0000000000000000 DR1: 0000000000000000 DR2: 000000000000000000		
			DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 00000000000000400		
			Call Trace:		
			<task></task>		
			tcp_cleanup_rbuf+0x3e7/ 0x4b0 net/ipv4/tcp.c:1493		
			mptcp_rcv_space_adjust net/mptcp/protocol.c:2085 [inline]		
			mptcp_recvmsg+0x2156/0x 2600		
			net/mptcp/protocol.c:2289		
			inet_recvmsg+0x469/0x6a0 net/ipv4/af_inet.c:885		
			sock_recvmsg_nosec net/socket.c:1051 [inline]		
			sock_recvmsg+0x1b2/0x25 0 net/socket.c:1073		
			sys_recvfrom+0x1a5/0x2 e0 net/socket.c:2265		
			do_sys_recvfrom net/socket.c:2283 [inline]		
			se_sys_recvfrom net/socket.c:2279 [inline]		
			x64_sys_recvfrom+0xe0/0 x1c0 net/socket.c:2279		
			do_syscall_x64 arch/x86/entry/common.c: 52 [inline]		

0-1

1-2

2-3

5-6 6-7

7-8 8-9

8-9 **9-1**0

3-4

	Description & CVE ID	Patch	NCIIPC ID
	do_syscall_64+0xcd/0x250 arch/x86/entry/common.c: 83		
	entry_SYSCALL_64_after_hw frame+0x77/0x7f		
	RIP: 0033:0x7feb5d857559		
	Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 51 18 00 00 90 48 89 f8 48		
	89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d		
	01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48		
	RSP: 002b:00007feb5d7f1208 EFLAGS: 00000246 ORIG_RAX: 0000000000002d		
	RAX: ffffffffffffffda RBX: 00007feb5d8e1318 RCX: 00007feb5d857559		
	RDX: 000000800000000e RSI: 0000000000000000 RDI: 00000000000000003		
	RBP: 00007feb5d8e1310 R08: 0000000000000000 R09: fffffff81000000		
	R10: 00000000000000000 R11: 0000000000000246 R12: 00007feb5d8e131c		
	R13: 00007feb5d8ae074 R14: 000000800000000e R15: 00000000fffffdef		
	and provided a nice reproducer.		

0-1

1-2

Page **750** of **1137**

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The root cause is the current bad handling of racing disconnect.		
			After the blamed commit below, sk_wait_data() can return (with		
			error) with the underlying socket disconnected and a zero rcv_mss.		
			Catch the error and return without performing any additional		
			operations on the current socket.		
			CVE ID : CVE-2024-53123		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/2 01fb9e1 64a1e4c	
			pmdomain: imx93-blk-ctrl: correct remove path	5937de2 cf58bcb 0327c08	
Always- Incorrect			The check condition should be 'i < bc-	664f, https:// git.kerne	
Control Flow	04-Dec-2024	5.5	>onecell_data.num_domains ', not	l.org/sta ble/c/8f	O-LIN-LINU- 241224/1573
Implement ation			'bc- >onecell_data.num_domains ' which will make the look never finish	c228ab5 d38a026 eae7183 a5f74a4f	,
			and cause kernel panic.	ac43d9b 6a,	
			Also disable runtime to address	https:// git.kerne l.org/sta	
			"imx93-blk-ctrl 4ac10000.system-	ble/c/f7 c7c5aa5	
CVSSv3 Scoring	Scale 0-1	1-2 2	- 3 3-4 4-5 5-6	56378a2	8-9 9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller: Unbalanced pm_runtime_enable!" CVE ID : CVE-2024-53134	c8da72c 1f7f238 b6648f9 5fb	
			In the Linux kernel, the following vulnerability has been resolved:		
			net/mlx5e: kTLS, Fix incorrect page refcounting	https:// git.kerne l.org/sta ble/c/2	
			The kTLS tx handling code is using a mix of get_page() and	723e8b2 cbd486c b96e5a6	
			page_ref_inc() APIs to increment the page reference. But on the release	1b2247 3f7fd62 e18df, https:// git.kerne	
N/A	04-Dec-2024	5.5	path (mlx5e_ktls_tx_handle_resy nc_dump_comp()), only put_page() is used.	l.org/sta ble/c/6 9fbd07f 17b0fda f8970bc	O-LIN-LINU- 241224/1574
			This is an issue when using pages from large folios: the get_page() references are stored on the folio page while the page_ref_inc()	705f5bf 115c297 839d, https:// git.kerne l.org/sta ble/c/9	
			references are stored directly in the given page. On release the folio	3a14620 b97c911 489a5b0 08782f3	
			page will be dereferenced too many times.	d9b0c4a eff4	
			This was found while doing kTLS testing with sendfile() + ZC when the		

3-4 4-5

5-6

6-7

9-10

1-2

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			served file was read from NFS on a kernel with NFS large folios support		
			(commit 49b29a573da8 ("nfs: add support for large folios")).		
			CVE ID : CVE-2024-53138		
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netlink: terminate outstanding dump on socket close Netlink supports iterative dumping of data. It provides the families the following ops: - start - (optional) kicks off the dumping process - dump - actual dump helper, keeps getting called until it returns 0 - done - (optional) pairs with .start, can be used for cleanup The whole process is asynchronous and the repeated calls to .dump don't actually happen in a tight loop, but rather are triggered in response to recvmsg() on the socket.	https:// git.kerne l.org/sta ble/c/1 14a61d8 d94ae3a 43b824 46cf737f d75702 1b834, https:// git.kerne l.org/sta ble/c/1 76c41b3 ca9281a 9736b6 7c6121b 03dbf0c 8c08f, https:// git.kerne l.org/sta ble/c/1 904fb9e bf91144 1f90a68 e96b22a a73e441 0505	O-LIN-LINU- 241224/1575

0-1

1-2

2-3

5-6 6-7 8-9

7-8

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This gives the user full control over the dump, but also means that		
			the user can close the socket without getting to the end of the dump.		
			To make sure .start is always paired with .done we check if there		
			is an ongoing dump before freeing the socket, and if so call .done.		
			The complication is that sockets can get freed from BH and .done		
			is allowed to sleep. So we use a workqueue to defer the call, when		
			needed.		
			Unfortunately this does not work correctly. What we defer is not		
			the cleanup but rather releasing a reference on the socket.		
			We have no guarantee that we own the last reference, if someone		
			else holds the socket they may release it in BH and we're back		
			to square one.		
			The whole dance, however, appears to be unnecessary. Only the user		

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
			can interact with dumps, so we can clean up when socket is closed.		
			And close always happens in process context. Some async code may		
			still access the socket after close, queue notification skbs to it etc.		
			but no dumps can start, end or otherwise make progress.		
			Delete the workqueue and flush the dump state directly from the release		
			handler. Note that further cleanup is possible in -next, for instance		
			we now always call .done before releasing the main module reference,		
			so dump doesn't have to take a reference of its own.		
			CVE ID : CVE-2024-53140		
Affected Ver	sion(s): From (i	ncluding)	6.7 Up to (excluding) 6.11.11		
			In the Linux kernel, the following vulnerability has been resolved:	https:// git.kerne l.org/sta ble/c/1	
N/A	06-Dec-2024	7.8	netfilter: ipset: add missing range check in bitmap_ip_uadt	579483 5378ed5 6fb9bac c6a5dd3 b9f3352	O-LIN-LINU- 241224/1576
			When tb[IPSET_ATTR_IP_TO] is not present but tb[IPSET_ATTR_CIDR] exists,	0604e, https:// git.kerne l.org/sta ble/c/3	
CVSSv3 Scoring *stands for all y		1-2 2	<mark>-3</mark> 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
			the values of ip and ip_to are slightly swapped. Therefore, the range check for ip should be done later, but this part is missing and it seems that the vulnerability occurs. So we should add missing range checks and remove unnecessary range checks. CVE ID : CVE-2024-53141	5f56c55 4eb1b56 b77b3cf 197a6b0 0922d4 9033d, https:// git.kerne l.org/sta ble/c/3c 20b594 8f119ae 61ee35a d8584d 666020c 91581	
Out-of- bounds Write	06-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: initramfs: avoid filename buffer overrun The initramfs filename field is defined in Documentation/driver- api/early-userspace/buffer- format.rst as: 37 cpio_file := ALGN(4) + cpio_header + filename + "\0" + ALGN(4) + data 55 ===== 56 Field name Field size Meaning	https:// git.kerne l.org/sta ble/c/1a 423bbbe af9e3e2 0c46865 01efd9b 661fe83 4db, https:// git.kerne l.org/sta ble/c/4 9d01e73 6c30453 19e030d 1e75fb9 83011ab aca7, https:// git.kerne l.org/sta ble/c/bb 7ac9667 0ab1d8d 681015f 9d66e45	0-LIN-LINU- 241224/1577

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			57 ======= =============================	dad579a f4d	
			 70 c_namesize 8 bytes		
			Length of filename, including final \0		
			When extracting an initramfs cpio archive, the kernel's do_name() path handler assumes a zero-		
			terminated path at @collected, passing it directly to filp_open() /		
			init_mkdir() / init_mknod().		
			If a specially crafted cpio entry carries a non-zero- terminated filename		
			and is followed by uninitialized memory, then a file may be created with		
			trailing characters that represent the uninitialized memory. The ability		
			to create an initramfs entry would imply already having full control of		
			the system, so the buffer overrun shouldn't be considered a security		
			vulnerability. Append the output of the		
			following bash script to an existing initramfs		

0-1

1-2

2-3

Page 757 of 1137

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and observe any created /initramfs_test_fname_over runAA* path. E.g.		
			./reproducer.sh gzip >> /myinitramfs		
			It's easiest to observe non- zero uninitialized memory when the output is		
			gzipped, as it'll overflow the heap allocated @out_buf in gunzip(),		
			rather than the initrd_start+initrd_size block.		
			reproducer.sh		
			nilchar="A" # change to "\0" to properly zero terminate / pad		
			magic="070701"		
			ino=1		
			mode=\$((0100777))		
			uid=0		
			gid=0		
			nlink=1		
			mtime=1		
			filesize=0		
			devmajor=0		
			devminor=1		
			rdevmajor=0		
			rdevminor=0		
			csum=0		
			fname="initramfs_test_fnam e_overrun"		

0-1

1-2

2-3

4-5

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			namelen=\$((\${#fname} + 1)) # plus one to account for terminator		
			printf "%s%08x%08x%08x%08x %08x%08x%08x%08x%08 x%08x%08x%08x%08x%s " \		
			\$magic \$ino \$mode \$uid \$gid \$nlink \$mtime \$filesize \		
			\$devmajor \$devminor \$rdevmajor \$rdevminor \$namelen \$csum \$fname		
			termpadlen=\$((1 + ((4 - ((110 + \$namelen) & 3)) % 4)))		
			printf "%.s\${nilchar}" \$(seq 1 \$termpadlen)		
			reproducer.sh		
			Symlink filename fields handled in do_symlink() won't overrun past the		
			data segment, due to the explicit zero-termination of the symlink		
			target.		
			Fix filename buffer overrun by aborting the initramfs FSM if any cpio		
			entry doesn't carry a zero- terminator at the expected (name_len - 1)		

0-1

1-2

2-3 3-4 4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Descri	otion & CVE ID		Ра	tch	NCIIF	PC ID
			offset. CVE ID : CV	/E-2024-531	42				
Vendor: Mic	Vendor: Microsoft								
Product: wi	ndows								
Affected Ver	sion(s): -								
Integer Underflow (Wrap or Wraparoun d)	10-Dec-2024	7.8	and earlier an Integer (Wrap or V vulnerabili result in ar execution i the current Exploitatio requires us	Vraparound) ty that could bitrary code n the context t user. n of this issue ser interaction m must open	by of e n in	obe. /sec y/pi cts/ ge/a 24-	ox.ad com curit codu brid	O-MIC-V 241224	
			CVE ID : CV	/E-2024-539	55				
Heap- based Buffer Overflow	10-Dec-2024	7.8	24.6.3 and affected by Buffer Over vulnerabili result in ar execution i the current Exploitatio requires us that a victin malicious f	a Heap-based rflow ty that could bitrary code n the context t user. n of this issue ser interaction m must open	d of e n in a	obe. /sec y/pr cts/ mier ro/a 24-	x.ad com curit codu pre re_p	O-MIC-V 241224	
Stack- based Buffer Overflow	10-Dec-2024	7.8	earlier are Stack-base Overflow v could resul code execu context of t Exploitatio	020.7, 2022.5 affected by a d Buffer ulnerability t t in arbitrary	hat ser.	obe. /sec y/pi cts/	ox.ad com curit codu fram ker/	0-MIC-V 241224	
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4	4-5 5-6	F	5-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			that a victim must open a malicious file.	106.htm l		
			CVE ID : CVE-2024-53959			
Product: wi	ndows_10_150	7				
Affected Ver	sion(s): * Up to	(excluding	g) 10.0.10240.20857			
Heap- based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138	https:// msrc.mi crosoft.c om/upd ate- guide/v ulnerabi lity/CVE -2024- 49138	O-MIC-WIND- 241224/1581	
	ndows_10_160					
Affected Ver	sion(s): * Up to	(excluding	g) 10.0.14393.7606			
Heap- based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138	https:// msrc.mi crosoft.c om/upd ate- guide/v ulnerabi lity/CVE -2024- 49138	O-MIC-WIND- 241224/1582	
Product: wi	ndows_10_180	9				
Affected Ver	sion(s): * Up to	(excluding	g) 10.0.17763.6659			
Heap- based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138	https:// msrc.mi crosoft.c om/upd ate- guide/v ulnerabi lity/CVE -2024- 49138	O-MIC-WIND- 241224/1583	
Product: windows_10_21h2						
Troutet. WI						

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Ver	Affected Version(s): * Up to (excluding) 10.0.19044.5247							
Heap- based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138	https:// msrc.mi crosoft.c om/upd ate- guide/v ulnerabi lity/CVE -2024- 49138	O-MIC-WIND- 241224/1584			
Product: wi	ndows_10_22h	2		1				
Affected Ver	sion(s): * Up to	(excluding	g) 10.0.19045.5247					
Heap- based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138	https:// msrc.mi crosoft.c om/upd ate- guide/v ulnerabi lity/CVE -2024- 49138	O-MIC-WIND- 241224/1585			
	ndows_11_22h							
Affected Ver	sion(s): * Up to	(excluding	g) 10.0.22621.4602	1				
Heap- based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138	https:// msrc.mi crosoft.c om/upd ate- guide/v ulnerabi lity/CVE -2024- 49138	O-MIC-WIND- 241224/1586			
Product: wi	ndows_11_23h	2						
Affected Ver	Affected Version(s): * Up to (excluding) 10.0.22631.4602							
Heap- based	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability	https:// msrc.mi crosoft.c	O-MIC-WIND- 241224/1587			
CVSSv3 Scoring *stands for all v		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 Overflow			CVE ID : CVE-2024-49138	om/upd ate- guide/v ulnerabi lity/CVE -2024- 49138	
	ndows_11_24h				
Affected Ver	sion(s): * Up to	(excluding	g) 10.0.26100.2605		
Heap- based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138	https:// msrc.mi crosoft.c om/upd ate- guide/v ulnerabi lity/CVE -2024- 49138	O-MIC-WIND- 241224/1588
Product: wi	ndows_server_	2008			
Affected Ver	sion(s): -				
Heap- based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138	https:// msrc.mi crosoft.c om/upd ate- guide/v ulnerabi lity/CVE -2024- 49138	O-MIC-WIND- 241224/1589
Affected Ver	sion(s): r2				
Heap- based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138	https:// msrc.mi crosoft.c om/upd ate- guide/v ulnerabi lity/CVE	O-MIC-WIND- 241224/1590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
				-2024- 49138		
Affected Vers	sion(s): sp2					
Heap- based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138	https:// msrc.mi crosoft.c om/upd ate- guide/v ulnerabi lity/CVE -2024- 49138	O-MIC-WIND- 241224/1591	
Product: wi	ndows_server_	2012				
Affected Vers	sion(s): -					
Heap- based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138	https:// msrc.mi crosoft.c om/upd ate- guide/v ulnerabi lity/CVE -2024- 49138	O-MIC-WIND- 241224/1592	
Affected Vers	sion(s): r2					
Heap- based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138	https:// msrc.mi crosoft.c om/upd ate- guide/v ulnerabi lity/CVE -2024- 49138	O-MIC-WIND- 241224/1593	
Product: windows_server_2016						
Affected Version(s): * Up to (excluding) 10.0.14393.7606						

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Heap- based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138	https:// msrc.mi crosoft.c om/upd ate- guide/v ulnerabi lity/CVE -2024- 49138	O-MIC-WIND- 241224/1594			
Product: wi	ndows_server_	2019						
Affected Ver	sion(s): * Up to	(excluding	g) 10.0.17763.6659					
Heap- based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138	https:// msrc.mi crosoft.c om/upd ate- guide/v ulnerabi lity/CVE -2024- 49138	O-MIC-WIND- 241224/1595			
Product: wi	ndows_server_	2022						
Affected Ver	sion(s): * Up to	(excluding	g) 10.0.20348.2966					
Heap- based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138	https:// msrc.mi crosoft.c om/upd ate- guide/v ulnerabi lity/CVE -2024- 49138	O-MIC-WIND- 241224/1596			
Product: windows_server_2022_23h2								
Affected Version(s): * Up to (excluding) 10.0.25398.1308								
Heap- based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138	https:// msrc.mi crosoft.c om/upd ate-	O-MIC-WIND- 241224/1597			
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10			

			guide/v ulnerabi lity/CVE -2024- 49138				
ndows_server_	2025						
sion(s): * Up to	(excluding	g) 10.0.26100.2605					
12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138	https:// msrc.mi crosoft.c om/upd ate- guide/v ulnerabi lity/CVE -2024- 49138	O-MIC-WIND- 241224/1598			
enatom							
enharmony							
sion(s): * Up to	(including	g) 4.0					
03-Dec-2024	5.5	in OpenHarmony v4.0.0 and prior versions allow a local attacker cause information leak through out-of-bounds Read. CVE ID : CVE-2024-12082	https:// gitee.co m/open harmon y/securi ty/blob/ master/ zh/secur ity- disclosu re/2024 /2024- 12.md	O-OPE-OPEN- 241224/1599			
Affected Version(s): * Up to (including) 4.1.1							
03-Dec-2024	8.8	in OpenHarmony v4.1.1 and prior versions allow a local attacker cause the common permission is upgraded to root through use after free. CVE ID : CVE-2024-10074	https:// gitee.co m/open harmon y/securi ty/blob/ master/	O-OPE-OPEN- 241224/1600			
	sion(s): * Up to 12-Dec-2024 enatom enharmony sion(s): * Up to 03-Dec-2024 sion(s): * Up to	12-Dec-2024 7.8 enatom enharmony sion(s): * Up to (including 03-Dec-2024 5.5	sion(s): * Up to (excluding) 10.0.26100.2605 12-Dec-2024 7.8 Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138 enatom enharmony sion(s): * Up to (including) 4.0 03-Dec-2024 5.5 in OpenHarmony v4.0.0 and prior versions allow a local attacker cause information leak through out-of-bounds Read. CVE ID : CVE-2024-12082 sion(s): * Up to (including) 4.1.1 03-Dec-2024 8.8 in OpenHarmony v4.1.1 and prior versions allow a local attacker cause information leak through out-of-bounds Read. CVE ID : CVE-2024-12082	-2024- 49138ndows_server_2025sion(s): * Up to (excluding) 10.0.26100.260512-Dec-20247.8Windows Common Log File System Driver Elevation of Privilege Vulnerability CVE ID : CVE-2024-49138https:// msrc.mi crosoft.c om/upd ate- guide/v ulnerability CVE ID : CVE-2024-49138enatomenatomenatom(s): * Up to (including) 4.0https:// gitee.co m/open lattacker cause information leak through out-of-bounds Read. CVE ID : CVE-2024-12082https:// gitee.co m/open harmon y/securi ty/blob/ mster/ zh/securi ity-03-Dec-20248.8in OpenHarmony v4.0.0 and prior versions allow a local attacker cause information leak through out-of-bounds Read. CVE ID : CVE-2024-12082https:// gitee.co m/open harmon y/securi ty/blob/ mster/ zh/securi ity- disclosu re/2024 /2024- 12.md			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				zh/secur ity- disclosu re/2024 /2024- 12.md	
Out-of- bounds Read	03-Dec-2024	5.5	in OpenHarmony v4.1.1 and prior versions allow a local attacker cause information leak through out-of-bounds Read. CVE ID : CVE-2024-9978	https:// gitee.co m/open harmon y/securi ty/blob/ master/ zh/secur ity- disclosu re/2024 /2024- 12.md	O-OPE-OPEN- 241224/1601
Vendor: Qua	alcomm				
Product: 20	5_mobile_plat	form_firm	iware		
Affected Vers	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-205 241224/1602
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	0-QUA-205 241224/1603
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Improper Improper Inproper Validation of Array IndexRaff and a consist and a consis	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
Affected Version(s): -Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua lcomm.c om/pro duct/pu blicreso ucres/se curitybu letin/de c2024- 2024- bulletin. htmlProduct: 315_5g_iot_modem_firmwareAffected Version(s): -Memory corruption while configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu letin/de configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044o-QUA-315- 241224/1605Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua lcomm.c om/pro					lletin/de cember- 2024- bulletin.						
Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// doc.nu our/tybu letin.n/de cember- 		-									
Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-430523docs.qua lcomm.c ources/se curitybu lletin/de0-QUA-215-2 241224/1604Product: 315-5g.iot_mode EVENDEImproper volumeMemory corruption while commerce 2024- bulletin. htmlhttps:// docs.qua lcomm.c om/pro duct/pu letin/de0-QUA-215-2 241224/1604Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu lletin/de cember- 2024- bulletin.Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua lcomm.c om/pro duct/pu letin/de cember- 2024- bulletin.Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua lcomm.c om/pro	Affected Ver	sion(s): -			https://						
Affected Version(s): -Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-315 0-QUA-315Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua lcomm.c om/pro	Input	02-Dec-2024	7.8	processing API calls to NPU with invalid input.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•					
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlhttps:// docs.qua lcomm.c ources/se curitybu lletin/de cember- 2024- bulletin. htmlBuffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition 			m_firmw	are							
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044docs.qua locures verses curitybu letin/de comber- 2024- bulletinQUA-315 41224/1605Buffer Over-read02-Dec-20248.4Memory corruption when entry in an SMEM partition on innuously.https:// acc.qua on/pro	Affected Ver	sion(s): -			1						
Buffer Over-read02-Dec-20248.4allocating and accessing an entry in an SMEM partition continuously.Inteps.// docs.qua lcomm.c om/pro0-QUA-315 241224/1606	Validation of Array	02-Dec-2024	8.4	Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•					
		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro	•					

Buffer Over-readO2-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition CVE ID : CVE-2024-33056blicreso urres/se ourres/seO-QUA-9205- 241224/1607Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition CVE ID : CVE-2024-33056O-QUA-9205- 241224/1607Product: 9205_Ite_modem_IrrewareVVIttps:// docs.qua lcomm.c om/pro duct/pu blicreso urres/se CVE ID : CVE-2024-33056O-QUA-9205- 241224/1607Product: 9205_Ite_modem_IrrewareVVIttps:// docs.qua lcomm.c on/pro duct/pu blicreso urres/se CVE ID : CVE-2024-33056O-QUA-9205- 241224/1607Product: 9205_Ite_modem_IrrewareVVIttps:// CVE ID : CVE-2024-33056O-QUA-9206- 241224/1607Product: 9207_Ite_modem_IrrewareVNNNNProduct: 9207_Ite_modem_IrrewareVVIttps:// Ittp:// Lettin/ http:// CVE ID : CVE-2024-33056O-QUA-9206- 241224/1608Product: 9207_Ite_modem_IrrewareVVIttp:// Ittp:// Ittp:// Lettin/ http:// CVE ID : CVE-2024-33056O-QUA-9206- 241224/1608Product: 9207_Ite_modem_IrrewareVVIttp:// <th>Weakness</th> <th>Publish Date</th> <th>CVSSv3</th> <th>Description & CVE ID</th> <th>Patch</th> <th>NCIIPC ID</th>	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Version(s): -Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition 					urces/se curitybu lletin/de cember- 2024- bulletin.				
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu bletin/de cember- 2024- bulletin. html0-QUA-9205- 241224/1607Product: 920-lte_modem_tirmwareImage: particitant state 			_firmwar	'e					
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition (CVE ID : CVE-2024-33056)docs.qua icomm.c on/pro buildein, de cember- 2024. buildein, https:// Memory corruption when https:// Memory corruption when https:// Memory corruption when allocating and accessing an intress/se to 204-2005 urress/se to 204-2006Product: 92-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// allocating and accessing an entry in an SMEM partition of allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// allocating and accessing an entry in an SMEM partition of allocating and accessing an entry in an SMEM partition allocating and accessing an entry in an SMEM partition of allocating and accessing an entry in an SMEM partition allocating and accessing an entry in an SMEM partition allocating and accessing an entry in an SMEM partition allocating and accessing and entry in an SMEM partition allocating and accessing an entry in an SMEM partition allocating and accessing an entry in an	Allected ver								
Affected Version(s): -Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlProduct: 920-zurotem-termeter9-QUA-9206- urces/se curitybu lletin/de cember- 2024- bulletin. html	Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.docs.qua icomm.c om/pro blicreso urces/se curitybu lletin/de 2024- bulletin.docs.qua icom.c om/pro blicreso urces/se curitybu lletin/de								
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-9206- 241224/1608Product: 920-2022 James J	Product: 92	06_lte_modem	_firmwar	re					
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056docs.qua Icomm.c om/pro Uurces/se Iletin/de CO24- Dulletin. Hulletin. Hulletin.Product: 92-7-10-20048.48.4Amory corruption when allocating and accessing an entry in an SMEM partition COE ID : CVE-2024-33056Idecs.qua Hulletin. Hulletin. Hulletin.Product: 92-7-10-20049-000-900-900-900-900-900-900-900-900-9	Affected Ver	sion(s): -							
		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•			
Affected Version(s): -	Product: 9207_lte_modem_firmware								
	Affected Version(s): -								

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-9207- 241224/1609
Product: ap	q8017_firmwa	re			
Affected Ver	sion(s): -				
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-APQ8- 241224/1610
Product: ap	q8037_firmwa	re			
Affected Ver	sion(s): -				
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-APQ8- 241224/1611

 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
				bulletin. html	
Product: aq	t1000_firmwa	re			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-AQT1- 241224/1612
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-AQT1- 241224/1613
Product: ar	8035_firmwar	e			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	O-QUA-AR80- 241224/1614

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-AR80- 241224/1615
	/2x_9150_firm	ware			
Affected Ver	sion(s): -			https://	
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-C-V2- 241224/1616
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	0-QUA-C-V2- 241224/1617

CVSSv3 Scoring Scale *stands for all versions

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			
				2024- bulletin. html				
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-C-V2- 241224/1618			
Product: cs	rb31024_firmv	vare						
Affected Ver	sion(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-CSRB- 241224/1619			
Product: fas	stconnect_6200)_firmwa	re					
Affected Ver	Affected Version(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	0-QUA-FAST- 241224/1620			

 CVSSv3 Scoring Scale
 0-1
 1-2
 2-3

 *stands for all versions

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1621
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1622
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-FAST- 241224/1623

Dece 774 of 1127

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1624
	stconnect_6700)_firmwa	re	·	
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1625
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-FAST- 241224/1626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1627
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1628
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1629
Product: fas	stconnect_6800	0_firmwa	re		
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 Ver	Affected Version(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1630					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1631					
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1632					

 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
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1633
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1634
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1635
Use After Free CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-FAST- 241224/1636 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33053	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1637
Product: fas	stconnect_6900)_firmwa	re	I	
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1638
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro duct/pu	0-QUA-FAST- 241224/1639

CVSSv3 Scoring Scale 0-1 *stands for all versions

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1640
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-FAST- 241224/1641
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	0-QUA-FAST- 241224/1642

CVSSv3 Scoring Scale *stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1643
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-FAST- 241224/1644
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1646
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1647
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-FAST- 241224/1648
Buffer Over-read CVSSv3 Scoring	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-FAST- 241224/1649 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: fas	stconnect_7800)_firmwa	re		
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1650
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1651
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call.	https:// docs.qua lcomm.c om/pro duct/pu	0-QUA-FAST- 241224/1652

CVSSv3 Scoring Scale *stands for all versions

0-1

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Descriptio	on & CVE ID	Pa	tch	NCIII	PC ID
			CVE ID : CVE	·2024-43048	blicr urce curit lletin cem 2024 bulle html	s/se cybu n/de ber- 4- etin.		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corr invoking IOC user space to private comm WLAN driver CVE ID : CVE	L calls from set generic and inside	lcom om/ duct blicr urce curit lletin	.qua im.c pro /pu reso s/se cybu n/de ber- 4- etin.	0-QUA- 241224	
Stack- based Buffer Overflow	02-Dec-2024	7.8	driver.	ΓL calls from	lcom om/ duct blicr	.qua im.c pro /pu reso s/se sybu n/de ber- 4- etin.	O-QUA- 241224	
Improper Input Validation CVSSv3 Scoring	02-Dec-2024 Scale 0-1	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052		lcom	.qua im.c pro /pu reso s/se cybu	0-QUA- 241224	

CVSSv3 Scoring Scale *stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1656
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-FAST- 241224/1657
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FAST- 241224/1659				
Product: flig	ght_rb5_5g_pla	tform_fir	mware						
Affected Ver	sion(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FLIG- 241224/1660				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FLIG- 241224/1661				
Product: fsr	Product: fsm10055_firmware								
CVSSv3 Scoring		1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10				
*stands for all v	versions		Dage 786 of 1127						

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Affected Ver	Affected Version(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FSM1- 241224/1662				
Product: fsr	n10056_firmw	vare							
Affected Ver	sion(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-FSM1- 241224/1663				
Product: ho	me_hub_100_p	latform_f	firmware						
Affected Ver	sion(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	O-QUA-HOME- 241224/1664				

CVSSv3 Scoring Scale0-11-22-33-44-55-66-7*stands for all versions

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				2024- bulletin. html				
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-HOME- 241224/1665			
Product: im	mersive_home	_214_pla	tform_firmware					
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-IMME- 241224/1666			
Product: immersive_home_216_platform_firmware								
Affected Ver	Affected Version(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	O-QUA-IMME- 241224/1667			

CVSSv3 Scoring Scale0-11-22-33-44-55-66-7*stands for all versions

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
				lletin/de cember- 2024- bulletin. html			
Product: im	mersive_home	-316_pla	tform_firmware				
Affected Vers	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-IMME- 241224/1668		
Product: im	mersive_home	-318_pla	tform_firmware				
Affected Vers	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-IMME- 241224/1669		
Product: immersive_home_3210_platform_firmware							
Affected Vers Buffer Over-read	sion(s): - 02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https:// docs.qua lcomm.c om/pro	O-QUA-IMME- 241224/1670		
				/1			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-IMME- 241224/1671
		e_326_pla	tform_firmware		
Affected Ver	sion(s): -			I	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-IMME- 241224/1672
Integer Overflow or Wraparoun d	02-Dec-2024 Scale 0-1	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https:// docs.qua lcomm.c om/pro duct/pu	O-QUA-IMME- 241224/1673 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html				
	q5010_firmwa	re						
Affected Ver	sion(s): -			1	[]			
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-IPQ5- 241224/1674								
Product: ip	q5028_firmwa	re						
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-IPQ5- 241224/1675			
Product: ipo	Product: ipq5300_firmware							
Affected Ver	sion(s): -							

5-6

6-7

7-8

8-9

Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs. urces/se curitybu literin/de cember- 2024- bulletin. httml0-QUA-IPQ5- 241224/1676Integer Overflow or Overflow d02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater that he ML IE inside which his element is present. CVE ID : CVE-2024-330630-QUA-IPQ5- 241224/1676Product: ipq5302_firmwareTransient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater that he ML IE inside which his element is present. CVE ID : CVE-2024-330630-QUA-IPQ5- 241224/1677Product: ipq5302_firmwareMemory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33066https:// docs.qua locember- 2024- bulletin. httml0-QUA-IPQ5- 241224/1677Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua locember- 2044-IPQ5- 241224/1678Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua locember 2024- bulletin. httmlProduct: ipq5312_firmware0122434455667788990	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparoun02-Dec-20247.5Fransient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which tis element is present. CVE ID : CVE-2024-33063docs.qua iom/pro duct/pu blicreso- 2024- 2024- bulletin.op-QUA-IPQ5- qu24/1677Product: retretretretretretretretreretretretretretretretreretretretretretretretretretretretretretr		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	
Affected Version(s): -Affected Version(s): -Buffer Over-read02-Dec-20248.4Nemory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056Product: ipt5312_firmware	Overflow or Wraparoun	02-Dec-2024	7.5	parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-IPQ5- 241224/1678Product: ipg5312_firmware	Product: ip	q5302_firmwa	re			
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. 	Affected Ver	sion(s): -				
	Over-read			allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	• •
CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Product: ipe	q5312_firmwa	re			
*stands for all versions	-		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): -	L			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-IPQ5- 241224/1679
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-IPQ5- 241224/1680
Product: ipc	15332_firmwa	re			
Affected Vers	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-IPQ5- 241224/1681
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
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-IPQ5- 241224/1682
Product: ipo	q6000_firmwa	re		·	
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-IPQ6- 241224/1683
Product: ipo	q6005_firmwa	re			
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-IPQ6- 241224/1684

 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		
				bulletin. html			
Product: ip	q6010_firmwa	re					
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-IPQ6- 241224/1685		
Product: ip	q6018_firmwa	re					
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-IPQ6- 241224/1686		
Product: ipq6028_firmware							
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	O-QUA-IPQ6- 241224/1687		
CVSSv3 Scoring *stands for all v		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			
				curitybu lletin/de cember- 2024- bulletin. html				
Product: ip	q8064_firmwa	re						
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-IPQ8- 241224/1688			
Product: ip	q8065_firmwa	re						
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-IPQ8- 241224/1689			
Product: ipq8068_firmware								
Affected Ver	sion(s): -							
				https://				
Buffer Over-read CVSSv3 Scoring	02-Dec-2024 Scale 0-1	8.4	Memory corruption when allocating and accessing an	docs.qua lcomm.c	0-QUA-IPQ8- 241224/1690 8-9 9-10			

Over-read02-Dec-20248.4entry in an SMEM partition continuously. CVE ID : CVE-2024-33056urces/se curitybu lletin/de 2024- bulletin. html241224/1691Product: ipq8070_firmwareAffected Version(s): -Memory corruption when allocating and accessing an entry in an SMEM partitionOurces/se curitybu lletin/de cember- 2024- bulletin. htmlProduct: ipq8070_firmwareMemory corruption when allocating and accessing an entry in an SMEM partition	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): -https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu letin/de cember- 2024- bulletin. httmlhttps:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu letin/de cember- 2024- bulletin. htmlo-QUA-IPQ8- 241224/1691Product: ipg8070_firmwareImage of the second				continuously.	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.			
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso 2024- bulletin, html0-QUA-IPQ8- 241224/1691Product: ipg8070_firmwareMemory corruption when allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua letin/de cember- 2024- 	Product: ip	q8070a_firmwa	are					
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056docs.qua icomm.c on/pro duct/pu blicreso 2024- bulletin. html0-QUA-IPQ8- 241224/1691Product: ipy8070_firmw=reMemory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua icomm.c om/pro 04uct/pu blicreso urces/se curitybu0-QUA-IPQ8- 241224/1691Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua icomm.c om/pro duct/pu blicreso urces/se curitybuBuffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua icomm.c om/pro duct/pu blicreso urces/se curitybuProduct: ipg8071a_firmw=reMemory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua icomm.c om/pro duct/pu blicreso urces/se curitybuProduct: ipg8071a_firmw=re8.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056docs.qua https:// docs.qua icommerc 2024- bulletin. https:// docs.qua icommerc and accessing an entry in an SMEM partition and accessing an entry in an SMEM partition and accessing an an and accessing an	Affected Ver	sion(s): -						
Affected Version(s): - Buffer 02-Dec-2024 8.4 Memory corruption when allocating and accessing an entry in an SMEM partition continuously. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-2024-bulletin. html 0-QUA-IPQ8-241224/1692 Product: ipq8071a_firmware Product: ipq8071a_firmware 0-QUA-IPQ8-241224/1692 0-QUA-IPQ8-241224/1692	Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/dedocs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de							
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-IPQ8- 241224/1692Product: ipq8071a_firmware	Product: ip	q8070_firmwa	re					
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056docs.qua lcomm.c oduct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmldocs.qua lcomm.c oduct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlProduct: ipterstructure	Affected Ver	sion(s): -						
	Buffer Over-read	02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	• •		
CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Product: ip	q8071a_firmwa	are	I				
	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 Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-IPQ8- 241224/1693
Product: ip	q8071_firmwa	re			
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-IPQ8- 241224/1694
Product: ip	q8072a_firmwa	are	I		
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	O-QUA-IPQ8- 241224/1695

CVSSv3 Scoring Scale0-11-22-33-4*stands for all versions

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
				2024- bulletin. html			
Product: ipo	<mark>q8072_firmwa</mark>	re		<u> </u>			
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-IPQ8- 241224/1696		
Product: ipo	q8074a_firmwa	are		1			
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-IPQ8- 241224/1697		
Product: ipq8074_firmware							
Affected Version(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	0-QUA-IPQ8- 241224/1698		
CVSSv3 Scoring *stands for all v		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
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
	18076a_firmwa	are			
Affected Vers	sion(s): -			1	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-IPQ8- 241224/1699
Product: ipc	<mark>18076_firmwa</mark>	re			
Affected Vers	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-IPQ8- 241224/1700
Product: ipc	18078a_firmwa	are	L	L	I
Affected Vers	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-IPQ8- 241224/1701
Product: ipo	q8078_firmwa	re		1	
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-IPQ8- 241224/1702
Product: ipe	q8173_firmwa	re			
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-IPQ8- 241224/1703

 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
				bulletin. html	
Product: ip	q8174_firmwa	re			
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-IPQ8- 241224/1704
Product: ip	q9008_firmwa	re		1	
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-IPQ9- 241224/1705
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	O-QUA-IPQ9- 241224/1706

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				cember- 2024- bulletin. html				
	q9554_firmwa	re						
Affected Ver	sion(s): -		I	1	1			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-IPQ9- 241224/1707			
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-IPQ9- 241224/1708			
Product: ipq9570_firmware								
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	O-QUA-IPQ9- 241224/1709			

CVSSv3 Scoring Scale0-11-22-33-44-55-66-7*stands for all versions

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybu lletin/de cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-IPQ9- 241224/1710
_	q9574_firmwa	re			
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-IPQ9- 241224/1711
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	O-QUA-IPQ9- 241224/1712

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Product: mdm8207_firmwære Hetin/de cember- 2024- bulletin. html Hetin/de cember- 2024- bulletin. html Affected Version(s): - Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056 https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html 0-QUA-MDM8- 241224/1713 Product: mdm92055_firmware Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056 https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. 0-QUA-MDM8- 241224/1713 Buffer Over-read 02-Dec-2024 8.4 Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056 https:// docs.qua lcomm.c om/pro 20-QUA-MDM9- 241224/1714 Product: mdm9250_firmwære K Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056 https:// docs.qua lcomm.c om/pro 0-QUA-MDM9- 241224/1714 Product: mdm9250_firmwære K Memory corruption when allocating and accessing an interver 0-QUA-MDM9- 241224/1714 Ruffer Over-read 02-Dec-2024 8.4 Memory corruption when allocating and accessing an interver 0-QUA-MDM9- 241224/1715	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): - Memory corruption when allocating and accessing an entry in an SMEM partition continuously. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin. /et continuously. 0-QUA-MDM8-241224/1713 Product: mdm9205s_firmware VF ID : CVE-2024-33056 https:// docs.qua lletin. /et comber-2024-3056 0-QUA-MDM8-241224/1713 Buffer Over-read 0.2-Dec-2024 8.4 Memory corruption when allocating and accessing an entry in an SMEM partition continuously. https:// docs.qua lletin. html 0-QUA-MDM9-241224/1713 Buffer Over-read 0.2-Dec-2024 8.4 Memory corruption when allocating and accessing an entry in an SMEM partition continuously. https:// docs.qua lleom.n. om/pro duct/pu blicreso urces/se urces/s					cember- 2024- bulletin.			
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se Curitybu lletin/de cember- 2024. bulletin. html0-QUA-MDM8- 241224/1713Product: mJm9205s_firmwareMemory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se0-QUA-MDM8- 241224/1713Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se0-QUA-MDM9- 241224/1714Product: mJm9250_firmwareMemory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se0-QUA-MDM9- 241224/1714Product: mJm9250_firmwareMemory corruption when allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua lcomm.c om/pro 20240-QUA-MDM9- 241224/1714Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an indicating and accessing an in	Product: mo	dm8207_firmw	are					
Buffer Over-read0.2-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056docs.qua letin/de cember- 2024- bulletin. html0-QUA-MDM8- 241224/1713Product: mJ9205s_firmJack Second Partition COULA-MDM8- 2024- bulletin. htmlMemory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso continuously. CVE ID : CVE-2024-33056oddocs.qua lcomm.c om/pro duct/pu blicreso continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso leitn/de continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu leitn/de curitybu leitn/de	Affected Ver	sion(s): -						
Affected Version(s): -Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-MDM9- 241224/1714Product: mJ250_firmAffected Version(s): -Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056Product: mJ250_firmWemory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056Product: mJ250_firmMemory corruption when allocating and accessing an illocating and accessing an allocating and accessing an illocating and accessing an illocating and accessing an illocating and accessing an02-Dec-20248.4Memory corruption when allocating and accessing an allocating and accessing an illocating and accessing an02-Dec-20248.42.43.44.55.66.77.88.99.10		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.			
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-MDM9- 241224/1714Product: m9250_firmw=reAffected Version (s) : -Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition curitybu lletin/de cember- 2024- bulletin. html0-QUA-MDM9- 241224/1714Product: m9250_firmw=reBuffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing anhttps:// docs.qua lcomm.c om/pro0-QUA-MDM9- 241224/1715	Product: mo	dm9205s_firm	ware					
Buffer Over-read02-Dec-20248.48.4Memory corruption when allocating and accessing an ontinuously. CVE ID : CVE-2024-33056docs.qua lom/pro duct/pu blicreso curitybu letin/de cember- 2024- bulletin. html0-QUA-MDM9- 241224/1714Product: m-7250_firmVE ID : CVE-2024-33056Nemory corruption when allocating and accessing an blicreso curitybu htmldocs.qua blicreso quebec-2024-300560-QUA-MDM9- 241224/1714Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an locating and accessing an allocating and accessing an on micro point in the state of the state o	Affected Ver	sion(s): -						
Affected Version(s): - Buffer 02-Dec-2024 8.4 Memory corruption when allocating and accessing an locating and accessing an locating and accessing an locating between the service of the	Over-read			allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	-		
Buffer Over-read 02-Dec-2024 8.4 Memory corruption when allocating and accessing an locating an locating an locating an locating an locating an locati								
	Buffer		8.4		docs.qua lcomm.c	•		
			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		
			entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html			
Product: me	dm9628_firmw	vare					
Affected Ver	sion(s): -						
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlO-QUA-MDM9- 241224/1716							
Product: me	dm9650_firmw	vare					
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-MDM9- 241224/1717		
Product: msm8108_firmware							
Product: m							
Affected Ver	sion(s): -						

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-MSM8- 241224/1718
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-MSM8- 241224/1719
Product: ms	sm8209_firmw	are			
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-MSM8- 241224/1720

Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua icomm.c ources/se curitybu lletin.de cember- 2024- bulletin. html0-QUA-MSM8- 241224/1721Product: msm8608_firm duffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c duft/pu blicresso0-QUA-MSM8- 241224/1722Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c duft/pu blicresso0-QUA-MSM8- 241224/1722Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duft/pu blicresso0-QUA-MSM8- 241224/1722Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua lcomm.c duft/pu blicressoProduct: msm8909v_firm CVSSV3 Scoring Scole041434455667788910	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): - Affected Version(s): - Buffer 02-Dec-2024 8.4 Memory corruption when allocating and accessing an entry in an SMEM partition com/product/publicreso urces/se continuously. https://docs.qua letin/de cember-2024-33056 0-QUA-MSM8-241224/1722 Improper 02-Dec-2024 8.4 Memory corruption when allocating and accessing an entry in an SMEM partition (cember-2024-bulletin. html https://docs.qua letin/de cember-2024-bulletin. html 0-QUA-MSM8-241224/1722 Improper 02-Dec-2024 7.8 Memory corruption while processing API calls to NPU with invalid input. https://docs.qua letin/de cember-2024-bulletin. html 0-QUA-MSM8-241224/1723 Validation 02-Dec-2024 7.8 Memory corruption while processing API calls to NPU with invalid input. https://docs.qua letin/de cember-2024-bulletin. html 0-QUA-MSM8-241224/1723 Validation 02-Dec-2024 7.8 Memory corruption while processing API calls to NPU with invalid input. https://docs.qua letin/de cember-2024-bulletin. html 0-QUA-MSM8-241224/1723 VSV3 Scoring Scale 04 14 24 34 45 56 6-7 78 89 910	Input	02-Dec-2024	7.8	processing API calls to NPU with invalid input.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•		
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso curitybu letin.de cember- 2024- bulletin. httmlhttps:// docs.qua lcomm.c om/pro duct/pu blicreso curitybu letin.de cember- 2024- bulletin. httmlo-QuA-MSM8- 241224/1722Improper Input Validation02-Dec-20247.8Memory corruption while 	-		are					
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.docs.qua lcomm.c om/pro duct/pu blicreso curitybu lletin/de cember- 2024- bulletin. html0-QUA-MSM8- 241224/1722Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu letin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu letin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu letin/de cember- 2024- bulletin. https:// docs.qua lcomm.c out/pro duct/pu blicreso urces/se curitybu letin/de cember- 2024- bulletin. https:// docs.qua lcomm.c blicreso urces/se curitybu letin/de cember- 2024- bulletin. https:// docs.qua lcomm.c blicreso urces/se urtybu letin/de cember- 2024- bulletin. https:// docs.qua lcomm.c blicreso urces/se urtybu letin/de cember- 2024- bulletin. https:// docs.qua lcomm.c blicreso urces/se urtybu letin/de cember- 2024- bulletin. https:// docs.qua lcomm.c blicreso urces/se urtybu letin/de cember- 2024- bulletin. https:// docs.qua lcomm.c docs.qua lcomm.c blicreso urces/se urtybu letin/de cember- 2024- bulletin. https:// docs.qua lcomm.c lcomm.c lcomm.c lcomm.c lcomm.c lcomm.c lcomm.c lcomm.c	Affected Ver	sion(s): -						
Improper Input Validation02-Dec-20247.8Remory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-MSM8- 241224/1723Product: msm890yw_firmwareCVSSv3 Scoring Scale0-1122-33-44-55-66-77-88-9910		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	-		
CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Input	02-Dec-2024	7.8	processing API calls to NPU with invalid input.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	e		
	Product: msm8909w_firmware							
*stands for all versions			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 Ver	Affected Version(s): -								
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-MSM8- 241224/1724				
Product: pn	n8937_firmwa	re							
Affected Ver	sion(s): -								
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-PM89- 241224/1725				
Product: pn	np8074_firmw	are							
Affected Ver	sion(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	O-QUA-PMP8- 241224/1726				

 CVSSv3 Scoring Scale
 0-1
 1-2
 2-3
 3-4

 *stands for all versions

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- bulletin. html	
-	m8255p_firmv	vare			
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAM8- 241224/1727
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAM8- 241224/1728
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-QAM8- 241224/1729

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
				bulletin. html	
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAM8- 241224/1730
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAM8- 241224/1731
-	m8295p_firmv	vare			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-QAM8- 241224/1732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAM8- 241224/1733
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAM8- 241224/1734
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAM8- 241224/1735

0-1

1-2

2-3

Page 812 of 1137

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAM8- 241224/1736
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAM8- 241224/1737
Product: qa	m8620p_firmv	vare			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAM8- 241224/1738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAM8- 241224/1739
_	m8650p_firmv	vare			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAM8- 241224/1740
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QAM8- 241224/1741

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
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAM8- 241224/1742
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAM8- 241224/1743
Product: qa	m8775p_firmv	ware			
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QAM8- 241224/1744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAM8- 241224/1745			
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAM8- 241224/1746			
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAM8- 241224/1747			
_	Product: qamsrv1h_firmware							
Affected Ver	sion(s): -							

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAMS- 241224/1748
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAMS- 241224/1749
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAMS- 241224/1750
Untrusted Pointer Dereferenc e CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the -3 3-4 4-5 5-6	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-QAMS- 241224/1751 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handle is not validated by the service. CVE ID : CVE-2024-33039	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qa	msrv1m_firmv	vare			
Affected Vers	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAMS- 241224/1752
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAMS- 241224/1753
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https:// docs.qua lcomm.c om/pro duct/pu 6-7 7-8	0-QUA-QAMS- 241224/1754 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QAMS- 241224/1755
-	a0000_firmwa	re			
Affected Ver	sion(s): -			https://	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA0- 241224/1756
Integer Overflow or Wraparoun d	02-Dec-2024 Scale 0-1	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	https:// docs.qua lcomm.c om/pro duct/pu blicreso	0-QUA-QCA0- 241224/1757 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Duodust: as	-1062 firmura		CVE ID : CVE-2024-33063	urces/se curitybu lletin/de cember- 2024- bulletin. html	
Affected Vers	a1062_firmwa	re			
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA1- 241224/1758
Product: qca	a1064_firmwa	re		•	
Affected Vers	sion(s): -				-
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA1- 241224/1759
Product: qca	a2062_firmwa	re		• 	
Affected Vers	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA2- 241224/1760
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA2- 241224/1761
Product: qc	a2064_firmwa	re		1	
Affected Ver	sion(s): -				
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA2- 241224/1762

Improper Restriction of Operations within the Bounds of a Memory Buffer0.2-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053https:// dcs.squa com/pro duct/pu blicreso curitybu lletin/dc cember- 2024- bulletin.0.2UA-QCA2- 241224/1763Product: qca2065_firmwareMemory corruption while information. CVE ID : CVE-2024-43053https:// dcs.squa Loom.c om/pro duct/pu blicreso ucer/space0.2UA-QCA2- 241224/1763Stack- basef basef overflow0.2-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050https:// dcs.squa Loom.c om/pro duct/pu blicreso uces/sea urces/sea <th>Weakness</th> <th>Publish Date</th> <th>CVSSv3</th> <th>Description & CVE ID</th> <th>Patch</th> <th>NCIIPC ID</th>	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): -Stack- based Buffer Overflow02-Dec-20247.8Memory corruption while 	Restriction of Operations within the Bounds of a Memory Buffer			invoking IOCTL calls from user space to read WLAN target diagnostic information.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.			
Stack- based Buffer Overflow02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050https:// docs.qua lcomm.c om/pro duct/pu blicreso curitybu lletin/de cember- 2024- bulletin. httmlhttps:// docs.qua lcomm.c om/pro duct/pu blicreso ures/se curitybu lletin/de cember- 2024- bulletin. httml0-QUA-QCA2- 241224/1764Improper Restriction of Operations within the Bounds of a Memory Buffer0-2-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053https:// docs.qua lcomm.c oduct/pu blicreso ures/se curitybu lletin/de cember- 2024- bulletin. httml0-QUA-QCA2- 241224/1765Product: quezues7.8Memory corruption while information. 			re					
Stack- based Buffer Overflow02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050docs.qua lcompro duct/pu blicreso urces/se 2024- bulletin. html0-QUA-QCA2- 241224/1764Improper Restriction of Operations within the Bounds of a Memory Buffer02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053https:// docs.qua lcomm.c om/pro om/pro operations within the Bounds of a Memory Bufferhttps:// target diagnostic information. CVE ID : CVE-2024-43053https:// docs.qua lcomm.c om/pro operators ucces/se0-QUA-QCA2- 241224/1764Product: rezueteresueteresueteresueteresuete	Affected Ver	sion(s): -						
Improper Restriction of Operations within the Bounds of a Memory Buffer02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-QCA2- 241224/1765Product: qc2066_firmware	based Buffer	02-Dec-2024	7.8	invoking IOCTL calls from user space to issue factory test command inside WLAN driver.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	• •		
	Restriction of Operations within the Bounds of a Memory	02-Dec-2024	7.8	invoking IOCTL calls from user space to read WLAN target diagnostic information.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	• •		
CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Product: qca2066_firmware							
*stands for all versions			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 Version(s): -							
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA2- 241224/1766		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA2- 241224/1767		
Product: qc	a4004_firmwa	re					
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA4- 241224/1768		
CVSSv3 Scoring *stands for all v		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: qc	a4024_firmwa	re						
Affected Ver	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA4- 241224/1769			
Product: qc	a6164_firmwa	re						
Affected Ver	sion(s): -							
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1770			
Product: qca6174a_firmware								
Affected Version(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	0-QUA-QCA6- 241224/1771			
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10			

Over-read02-Dec-20248.4Citary in an synthy particular continuously.Urces/se curitybu llein/de cember- 2024- bulletin. html241224/177:Stack- based Buffer Overflow02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httml0-QUA-QCA6 241224/177Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu0-QUA-QCA6 241224/1773Stack- based Buffer Overflow02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se curitybu0-QUA-QCA6 241224/1773Improper Imput Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu0-QUA-QCA6 241224/1773					2024- bulletin.	
Stack- based Buffer Overflow02-Dec-20247.8Memory corruption while 		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	O-QUA-QCA6- 241224/1772
Improper Input02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input.docs.qua lcomm.c om/pro blicreso urces/se curitybu	based Buffer	02-Dec-2024	7.8	invoking IOCTL calls from user space to issue factory test command inside WLAN driver.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	0-QUA-QCA6- 241224/1773
CVE ID : CVE-2024-43052 lletin/de cember- 2024- bulletin. html		02-Dec-2024	7.8	processing API calls to NPU	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	O-QUA-QCA6- 241224/1774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1775			
Product: qc	a6174_firmwa	re						
Affected Ver	sion(s): -							
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1776			
Product: qca6310_firmware								
Affected Ver	sion(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-QCA6- 241224/1777			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				bulletin. html				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1778			
	a6320_firmwa	re						
Affected Ver	sion(s): -			1				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1779			
Product: qca6335_firmware								
Affected Version(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	0-QUA-QCA6- 241224/1780			

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1781
	a6391_firmwa	re			
Affected Ver	sion(s): -			T	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1782
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	0-QUA-QCA6- 241224/1783

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
				2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1784
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1785
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1786

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1787
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1788
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1789
Buffer Over-read CVSSv3 Scoring	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-QCA6- 241224/1790 8-9 9-10

Product: qca6420_firmwarevalidate the IPC message received from the firmware. CVE ID : CVE-2024-33037duct, blicr urce. curit lletin cemi 2024 bulle htmlProduct: qca6420_firmwareAffected Version(s): -Affected Version(s): -Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https: docs licr urce. curit lletin cemi 2024Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https: docs licr urce. curit lletin cemi 2024Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition urce.	reso es/se tybu	-
Affected Version(s): -Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https: 	ber- 4- etin.	s/se ybu a/de per- tin.
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https docs loid urce. curit lletin cemi 2024 bulle httpsBuffer Owen med02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partitionhttps		
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044docs lcom om/r urce. curit lletin cemi 2024 bulle htmlBuffer Orum med02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partitionhttps:		
Buffer 02-Dec-2024 8.4 entry in an SMEM partition docs	s.qua nm.c pro /pu reso s/se tybu n/de ber- 4- etin.	qua m.c pro /pu eso s/se ybu a/de per- tin.
Over-read continuously. curit CVE ID : CVE-2024-33056 lletin 2024 bulle html	s.qua nm.c pro /pu reso s/se tybu n/de ber- 4- etin.	qua m.c pro /pu eso s/se ybu a/de per- tin.
Stack- based Buffer Overflow 02-Dec-2024 7.8 Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. https: docs lcom om/r duct,	s.qua nm.c pro	qua m.c pro 0-QUA-QCA6- 241224/1793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2024-43050	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html						
	Product: qca6421_firmware									
Affected Ver	sion(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1794					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1795					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso	0-QUA-QCA6- 241224/1796					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qc	a6426_firmwa	re		·	
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1797
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1798
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	0-QUA-QCA6- 241224/1799

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
				curitybu lletin/de cember- 2024- bulletin. html	
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QCA6- 241224/1800
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1801
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-QCA6- 241224/1802
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				
				bulletin. html					
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1803				
Product: qca6428_firmware									
Affected Ver	sion(s): -			1					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1804				
Product: qca6430_firmware									
Affected Version(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	0-QUA-QCA6- 241224/1805				

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1806
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1807
	a6431_firmwa	re			
Affected Ver	sion(s): -			http://	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	0-QUA-QCA6- 241224/1808
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3 3-4 4-5 5-6</mark>	6-7 7-8	8-9 9-10

				2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1809
Improper Input (Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1810
Product: qca	6436_firmwa	re			
Affected Versi	on(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-QCA6- 241224/1811
CVSSv3 Scoring So	cale 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
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1812
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1813
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1814

Page 838 of 1137

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1815		
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1816		
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1817		
Product: qca6438_firmware							
Affected Ver	sion(s): -						

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1818		
Product: qca	a6554a_firmw	are					
Affected Vers	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1819		
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1820		
Product: qca6564au_firmware							
CVSSv3 Scoring		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10		
*stands for all v	resions		Page 9/0 of 1127				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Affected Ver	sion(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1821	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1822	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1823	
Product: qca6564a_firmware						
Affected Version(s): -						
CVSSv3 Scoring stands for all v		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
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1824
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1825
Product: qc	a6564_firmwa	re		1	
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1827
-	a6574au_firm	ware			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QCA6- 241224/1828
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1829

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
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1830
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1831
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1832
Buffer Over-read CVSSv3 Scoring	02-Dec-2024 Scale 0-1	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-QCA6- 241224/1833 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qc	a6574a_firmw	are		I	
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1834
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1835
Integer Overflow or Wraparoun d CVSSv3 Scoring	02-Dec-2024 Scale 0-1	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https:// docs.qua lcomm.c om/pro duct/pu 6-7 7-8	0-QUA-QCA6- 241224/1836 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
-	a6574_firmwa	re			
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1837
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1838
Integer Overflow or Wraparoun d	02-Dec-2024 Scale 0-1	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	https:// docs.qua lcomm.c om/pro duct/pu blicreso	0-QUA-QCA6- 241224/1839 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33063	urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qc	a6584au_firm	ware			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1840
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1841
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	0-QUA-QCA6- 241224/1842

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33063	curitybu lletin/de cember- 2024- bulletin. html	
-	a6595au_firmv	ware			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1843
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1844
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	O-QUA-QCA6- 241224/1845

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1846
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1847
Product: qca	a6595_firmwa	re		I	
Affected Vers	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	0-QUA-QCA6- 241224/1848
CVSSv3 Scoring		1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
*stands for all v	rersions		Dage 8/0 of 1127		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1849
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1850
	a6678aq_firm	ware			
Affected Vers	sion(s): -			https://	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	0-QUA-QCA6- 241224/1851
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3 3-4 4-5 5-6</mark>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1852
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1853
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QCA6- 241224/1854

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qc	a6688aq_firmv	ware		1	L
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1855
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1856
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1857
Product: qc	a6694_firmwa	re	I		
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 Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1858
•	a6696_firmwa	re			
Affected Ver	sion(s): -			T	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1859
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1860
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
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1861
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1862
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1863
Buffer Over-read CVSSv3 Scoring	02-Dec-2024 Scale 0-1	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-QCA6- 241224/1864 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qc	a6698aq_firm	ware			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1865
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1866
Integer Overflow or Wraparoun d CVSSv3 Scoring	02-Dec-2024 Scale 0-1	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https:// docs.qua lcomm.c om/pro duct/pu 6-7 7-8	0-QUA-QCA6- 241224/1867 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qca	a6777aq_firmv	ware		L	
Affected Vers	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QCA6- 241224/1868
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1869
Product: qca	a6787aq_firmv	ware		1	
Affected Vers	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https:// docs.qua lcomm.c	0-QUA-QCA6- 241224/1870
CVSSv3 Scoring *stands for all v		1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

CVE-2024-33056	om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	
	bulletin. html	
nt DOS while the ML IE when a with common info f the ML IE greater ML IE inside which nent is present. CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1871
	·	
	http://	
corruption while ring the SMR/S2CR in Bypass mode. CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA6- 241224/1872
ig and accessing an an SMEM partition	https:// docs.qua lcomm.c om/pro	0-QUA-QCA6- 241224/1873
	corruption while ing the SMR/S2CR in Bypass mode. CVE-2024-33044	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID : CVE-2024-33056	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html				
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QCA6- 241224/1874			
Product: qca	a8072_firmwa	re						
Affected Vers	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA8- 241224/1875			
	Product: qca8075_firmware							
Affected Vers	sion(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https:// docs.qua	0-QUA-QCA8- 241224/1876			
CVSSv3 Scoring *stands for all v		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
			entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA8- 241224/1877
	a8081_firmwa	re			
Affected Vers	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QCA8- 241224/1878
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https:// docs.qua lcomm.c	0-QUA-QCA8- 241224/1879
CVSSv3 Scoring *stands for all v		1-2 2	-3 3-44-55-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA8- 241224/1880
Product: qca	a8082_firmwa	re			
Affected Vers	sion(s): -				
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QCA8- 241224/1881
Product: qca	a8084_firmwa	re		·	
Affected Vers	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA8- 241224/1882
Product: qc	a8085_firmwa	re			
Affected Ver	sion(s): -				
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA8- 241224/1883
	a8337_firmwa	re			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-QCA8- 241224/1884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA8- 241224/1885
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA8- 241224/1886
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA8- 241224/1887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA8- 241224/1888
Product: qc	a8386_firmwa	re			
Affected Ver	sion(s): -				
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA8- 241224/1889
	a9377_firmwa	re			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-QCA9- 241224/1890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA9- 241224/1891
_	a9379_firmwa	re			
Affected Ver	sion(s): -			1	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCA9- 241224/1892
Product: qc	c2073_firmwa	re			
Affected Ver	sion(s): -				
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	0-QUA-QCC2- 241224/1893

CVSSv3 Scoring Scale0-11-22-33-44-55-66-7*stands for all versions

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCC2- 241224/1894
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCC2- 241224/1895
Product: qc	c2076_firmwa	re			
Affected Vers	sion(s): -				
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	0-QUA-QCC2- 241224/1896
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
				2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCC2- 241224/1897
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCC2- 241224/1898
Product: qcc	:710_firmware	è.			
Affected Vers	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-QCC7- 241224/1899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCC7- 241224/1900
Product: qc	f8000_firmwai	re		·	•
Affected Vers	sion(s): -			-	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCF8- 241224/1901
Product: qc	f8001_firmwai	re			
Affected Ver	sion(s): -				
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	0-QUA-QCF8- 241224/1902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				cember- 2024- bulletin. html				
Product: qc	m2150_firmwa	are						
Affected Ver	sion(s): -				_			
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCM2- 241224/1903			
Product: qc	m4325_firmwa	are						
Affected Ver	sion(s): -							
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QCM4- 241224/1904			
-	Product: qcm5430_firmware Affected Version(s): -							
			Momony committee subile	https://				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu	O-QUA-QCM5- 241224/1905			
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QCM5- 241224/1906
Product: qc Affected Ver	m6490_firmw	are			
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCM6- 241224/1907
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver.	https:// docs.qua lcomm.c om/pro duct/pu blicreso	O-QUA-QCM6- 241224/1908

4-5

5-6

6-7

7-8

8-9

9-10

3-4

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-43050	urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qc	m8550_firmwa	are		I	L
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCM8- 241224/1909
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCM8- 241224/1910
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	O-QUA-QCM8- 241224/1911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				curitybu lletin/de cember- 2024- bulletin. html				
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QCM8- 241224/1912			
	n5124_firmwa	re		·				
Affected Vers	sion(s): -			-				
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QCN5- 241224/1913			
-	Product: qcn6224_firmware							
Affected Vers	sion(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu	0-QUA-QCN6- 241224/1914			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html				
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCN6- 241224/1915			
	Product: qcn6274_firmware							
Affected Ver	sion(s): -				ſ			
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCN6- 241224/1916			
Integer Overflow or Wraparoun d	02-Dec-2024 Scale 0-1	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	https:// docs.qua lcomm.c om/pro duct/pu blicreso	O-QUA-QCN6- 241224/1917 8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: or	n6402_firmwa	10	CVE ID : CVE-2024-33063	urces/se curitybu lletin/de cember- 2024- bulletin. html	
Affected Vers					
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCN6- 241224/1918
	n6412_firmwa	re			
Affected Vers	sion(s): -			1	1
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCN6- 241224/1919
Product: qci	n6422_firmwa	re	I	<u> </u>	<u> </u>
Affected Vers	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCN6- 241224/1920	
Product: qc	n6432_firmwa	re		·		
Affected Ver	sion(s): -					
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCN6- 241224/1921	
Product: qcn7605_firmware						
Affected Ver	sion(s): -					
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-QCN7- 241224/1922	

 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

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			bulletin. html			
n7606_firmwa	re					
sion(s): -						
02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCN7- 241224/1923		
	re					
sion(s): -			T	1		
02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCN9- 241224/1924		
Product: qcn9011_firmware						
sion(s): -				I		
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso	0-QUA-QCN9- 241224/1925		
	n7606_firmwa sion(s): - 02-Dec-2024 02-Dec-2024 02-Dec-2024 02-Dec-2024	n7606_firmware sion(s): - 02-Dec-2024 7.8 n9000_firmware sion(s): - 02-Dec-2024 7.5 n9000_firmware sion(s): - 02-Dec-2024 7.5	n7606_firmwaresion(s): -02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050n9000_firmwaresion(s): -Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063n9011_firmwaresion(s): -02-Dec-20247.502-Dec-20247.5Memory corruption while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	n7606_firmwarebulletin. htmln7606_firmwarewemory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmln9000_firmwareTransient DOS while parsing the ML IE when a beacon with common info length of the ML IE inside which this element is present. CVE ID : CVE-2024-33063https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin. htmln9011_firmwareVE ID : CVE-2024-33063https:// docs.qua lcomm.c02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode.https:// docs.qua lcomm.c om/pro		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
				curitybu lletin/de cember- 2024- bulletin. html		
-	n9012_firmwa	re				
Affected Ver	sion(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCN9- 241224/1926	
Product: qc	n9024_firmwa	re				
Affected Ver	sion(s): -					
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCN9- 241224/1927	
Product: qcn9074_firmware						
Affected Ver	sion(s): -					
Integer Overflow or	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info	https:// docs.qua lcomm.c	0-QUA-QCN9- 241224/1928	
	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
Wraparoun d			length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCN9- 241224/1929
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCN9- 241224/1930
Buffer Over-read CVSSv3 Scoring	02-Dec-2024 Scale 0-1	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware.	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	0-QUA-QCN9- 241224/1931 8-9 9-10

Product: qcn9160_firmwareCVE ID : CVE-2024-33037curity lletin, cemb 2024- bullet htmlProduct: qcn9160_firmwareAffected Version(s): -Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https: docs.d corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https: docs.d icom om/p duct/ blicre urces curity lletin, continuously.Product: qcn9274_firmwareAffected Version(s): -Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https: docs.d lcom om/p duct/ blicre urces curity Iletin, cemb 2024-33044	tch	NCIIPC ID
Affected Version(s): -Affected Version(s): -Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https: docs.o. lcomr om/p duct/ blicre urces 2024- bulletin htmlProduct: qcn9274_firmware	n/de ber- 4- etin.	
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.https: docs.d lcomr om/pProduct: qcn9274_firmware8.4Memory corruption when allocating and accessing an entry in an SMEM partition 		
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056docs.o. loomr om/p duct/ blicre urces curity lletin, cemb 2024- bullet htmlProduct: qcr9274_firmwareVeride in the second	ci / /	
Affected Version(s): - https://docs.org/	a.qua nm.c pro /pu reso s/se tybu n/de ber- 4- etin.	0-QUA-QCN9- 241224/1932
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https: docs.c lcomr om/p duct/ blicre urces curity lletin, cemb 2024- bullet		
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044docs.d Icomr om/p duct/ Blicre Curity Iletin, cembr 2024- bullet		
html	a.qua nm.c pro /pu reso s/se tybu n/de ber- 4- etin.	0-QUA-QCN9- 241224/1933
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.https: docs.c Icomr om/pCVE ID : CVE-2024-33056duct/	.qua nm.c pro	0-QUA-QCN9- 241224/1934

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html			
02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCN9- 241224/1935		
02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCN9- 241224/1936		
Product: qcs2290_firmware						
Affected Version(s): -						
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	0-QUA-QCS2- 241224/1937		
	02-Dec-2024 02-Dec-2024	02-Dec-2024 7.8 02-Dec-2024 7.5 sz290_firmware 7.5	02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-4305202-Dec-20247.8Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063s2290_firmwareImage: CVE ID : CVE-2024-3306302-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua lcomm.c om/pro duct/pu bilicreso urces/se curitybu02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua lcomm.c om/pro duct/pu bilicreso urces/se curitybu02-Dec-20247.5Fransient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater this element is present. CVE ID : CVE-2024-33063https:// docs.qua lcomm.c om/pro duct/pu bilicreso urces/se curitybus2290_firmwareMemory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33065https:// docs.qua lcomm.c om/pro duct/pu		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: qc	s410_firmware	e			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS4- 241224/1938
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS4- 241224/1939
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	0-QUA-QCS4- 241224/1940

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
		to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	curitybu lletin/de cember- 2024- bulletin. html			
02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS4- 241224/1941		
02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS4- 241224/1942		
Product: qcs4290_firmware						
Affected Version(s): -						
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	0-QUA-QCS4- 241224/1943		
	02-Dec-2024 02-Dec-2024 02-Dec-2024	02-Dec-2024 6.7 02-Dec-2024 6.7 02-Dec-2024 6.1	outputto huge allocation or invalid memory access. CVE ID : CVE-2024-3303602-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-3305302-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-33037s4290_firmwareUo2-Dec-20248.402-Dec-20248.4	02-Dec-20246.7to huge allocation or invalid memory access. CVE ID : CVE-2024-330366curitybu lletin/de cember- 2024- bulletin. httm02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua lcomm.c om/pro duct/pu blicreso urres/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lletin/de cember- 2024- bulletin. httm02-Dec-20246.7Information disclosure as NPU firmware can send invalid IPC message received from the firmware. CVE ID : CVE-2024-33037https:// docs.qua lletin/de cember- 2024- bulletin. httm02-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-33037https:// docs.qua lletin/de cember- 2024- bulletin. httms4290_firmware8.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
-	s4490_firmwa	re		·	
Affected Ver	sion(s): -			1	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QCS4- 241224/1944
Product: qc	s5430_firmwa	re			
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QCS5- 241224/1945
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	0-QUA-QCS5- 241224/1946

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS5- 241224/1947
-	s610_firmware	9			
Affected Ver	sion(s): -			http://	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS6- 241224/1948
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	0-QUA-QCS6- 241224/1949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybu lletin/de cember- 2024- bulletin. html	
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS6- 241224/1950
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS6- 241224/1951
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-QCS6- 241224/1952
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					
				bulletin. html						
Product: qc	Product: qcs6125_firmware									
Affected Ver	sion(s): -									
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS6- 241224/1953					
Product: qc	s6490_firmwa	re		1						
Affected Ver	sion(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS6- 241224/1954					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	0-QUA-QCS6- 241224/1955					

4-5

5-6

6-7

7-8

8-9

9-10

3-4

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS6- 241224/1956
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS6- 241224/1957
	s7230_firmwa	re			
Affected Vers	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	0-QUA-QCS7- 241224/1958
CVSSv3 Scoring *stands for all v		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
				2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS7- 241224/1959
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS7- 241224/1960
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS7- 241224/1961

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Product: qc	Product: qcs8155_firmware								
Affected Ver	Affected Version(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS8- 241224/1962				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS8- 241224/1963				
Product: qc	s8250_firmwa	re		•					
Affected Ver	sion(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-QCS8- 241224/1964				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS8- 241224/1965
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS8- 241224/1966
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS8- 241224/1967
Product: qcs	s8550_firmwa	re			
CVSSv3 Scoring		1-2 2	<mark>-3</mark> 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 Ver	sion(s): -				L
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS8- 241224/1968
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QCS8- 241224/1969
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QCS8- 241224/1970
Integer Overflow	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a	https:// docs.qua	0-QUA-QCS8- 241224/1971

Weakness	Publish Date	CVSSv3	Des	cription & C	VE ID		Patch	NCII	PC ID
or Wraparoun d			length of than the this elen	vith comm f the ML IE ML IE insi nent is pre CVE-202 4	greater de whic sent.	or h du bl un cu lle ce 20 bu	omm.c n/pro act/pu icreso cces/se uritybu etin/de ember- 024- alletin.		
Product: qc	s9100_firmwa	re	•						
Affected Ver	sion(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Configur register	corruptio ing the SM in Bypass CVE-202 4	IR/S2CR mode.	da lc on du bl uu cu lla ce 20 bu	tps:// ocs.qua omm.c n/pro uct/pu icreso cces/se uritybu etin/de ember- 024- ulletin.	0-QUA- 241224	-
Buffer Over-read	02-Dec-2024	8.4	allocatin entry in continuc	corruptio g and acce an SMEM ously. CVE-202 4	essing an partition	da lc on du bl cu cu cu cu cu cu cu cu cu cu cu cu cu	tps:// ocs.qua omm.c n/pro act/pu icreso cces/se uritybu etin/de ember- 024- alletin.	0-QUA- 241224	
Product: qdu1000_firmware									
Affected Ver	sion(s): -								
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
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QDU1- 241224/1974
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QDU1- 241224/1975
Product: qd	u1010_firmwa	ire		1	
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QDU1- 241224/1976

 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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QDU1- 241224/1977
	u1110_firmwa	re			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QDU1- 241224/1978
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QDU1- 241224/1979
Product: qd	u1210_firmwa	re		·	
CVSSv3 Scoring		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10
*stands for all v	resions		Dage 802 of 1127		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): -	L			
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QDU1- 241224/1980
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QDU1- 241224/1981
Product: qd	x1010_firmwa	re			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QDX1- 241224/1982
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 Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QDX1- 241224/1983
	x1011_firmwa	re			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QDX1- 241224/1984
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QDX1- 241224/1985
Product: qe	p8111_firmwa	re		I	I
CVSSv3 Scoring		1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
*stands for all v	versions		Dago 905 of 1127		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QEP8- 241224/1986		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QEP8- 241224/1987		
Product: qe	t4101_firmwa	re					
Affected Vers	sion(s): -						
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QET4- 241224/1988		
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Affected Version	7 114_firmwa ion(s): - 02-Dec-2024	re 8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-QFW7- 241224/1989
Improper Validation of Array		8.4	Configuring the SMR/S2CR register in Bypass mode.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	
Validation of Array	02-Dec-2024	8.4	Configuring the SMR/S2CR register in Bypass mode.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QFW7- 241224/1990
Integer Overflow or (Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QFW7- 241224/1991
Product: qfw'	7124_firmwa	re		L	
CVSSv3 Scoring So stands for all ver		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 Version(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QFW7- 241224/1992		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QFW7- 241224/1993		
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QFW7- 241224/1994		
Product: qrb5165m_firmware							
	Affected Version(s): -						
CVSSv3 Scoring *stands for all v		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
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QRB5- 241224/1995
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QRB5- 241224/1996
Product: qr	b5165n_firmw	are		1	
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QRB5- 241224/1997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QRB5- 241224/1998
Product: qr	u1032_firmwa	re			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QRU1- 241224/1999
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QRU1- 241224/2000
Product: qr	u1052_firmwa	re			
CVSSv3 Scoring		1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
*stands for all v	versions		Dago 000 of 1127		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QRU1- 241224/2001		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QRU1- 241224/2002		
Product: qr	u1062_firmwa	re					
Affected Vers	sion(s): -						
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QRU1- 241224/2003		
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 Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QRU1- 241224/2004
-	m8250_firmwa	are			
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QSM8- 241224/2005
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QSM8- 241224/2006

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QSM8- 241224/2007
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QSM8- 241224/2008
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QSM8- 241224/2009
Buffer Over-read CVSSv3 Scoring	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-QSM8- 241224/2010 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: as	m8350_firmwa	are	validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Affected Ver					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-QSM8- 241224/2011
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QSM8- 241224/2012
	w8573_firmwa	ire		1	
Affected Ver	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QSW8- 241224/2013
Product: qt	s110_firmware			1	
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-QTS1- 241224/2014
Product: qx	m8083_firmwa	are			
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-QXM8- 241224/2015

 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					
				bulletin. html						
Product: ro	Product: robotics_rb3_platform_firmware									
Affected Ver	sion(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-ROBO- 241224/2016					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-ROBO- 241224/2017					
Product: ro	botics_rb5_pla	tform_fir	mware	<u> </u>						
Affected Ver	sion(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	O-QUA-ROBO- 241224/2018					

4-5

5-6

6-7

7-8

8-9

9-10

3-4

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				cember- 2024- bulletin. html				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-ROBO- 241224/2019			
	Product: sa2150p_firmware							
Affected Ver	sion(s): -			1				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA21- 241224/2020			
Product: sa4150p_firmware								
Affected Ver	sion(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	0-QUA-SA41- 241224/2021			

4-5

5-6

6-7

7-8

8-9

9-10

3-4

2-3

0-1

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA41- 241224/2022
4155p_firmwa	re			
sion(s): -				
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA41- 241224/2023
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	0-QUA-SA41- 241224/2024
	02-Dec-2024 4155p_firmwa sion(s): - 02-Dec-2024	02-Dec-2024 8.4 4155p_firmware sion(s): - 02-Dec-2024 8.4	Image: Constraint of the system of the sys	02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-202402-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-2024- bulletin. httml4155p_firmware02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-2024- bulletin. httml02-Dec-20248.4Memory corruption whele allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-2024- bulletin. httml

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Product: sa	6145p_firmwa	re			
Affected Ver	sion(s): -			T	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA61- 241224/2025
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA61- 241224/2026
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access.	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	0-QUA-SA61- 241224/2027

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33036	cember- 2024- bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA61- 241224/2028
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA61- 241224/2029
	6150p_firmwa	re			
Affected Ver	sion(s): -			http://	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	0-QUA-SA61- 241224/2030
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA61- 241224/2031
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA61- 241224/2032
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA61- 241224/2033

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
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA61- 241224/2034
	6155p_firmwa	re			
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA61- 241224/2035
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA61- 241224/2036

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
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA61- 241224/2037
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA61- 241224/2038
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA61- 241224/2039
Buffer Over-read CVSSv3 Scoring	02-Dec-2024 Scale 0-1	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-SA61- 241224/2040 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Product: sa	6155_firmward		validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html				
Affected Ver								
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua l.comm.c om/pro duct/pu blicreso urces/se curitybu lletin/de 2024- bulletin. htmlhttps:// docs.qua l.comm.c om/pro duct/pu blicreso urces/se curitybu								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA61- 241224/2042			
	7255p_firmwa	re		1				
Affected Ver	sion(s): -							

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA72- 241224/2043
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA72- 241224/2044
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA72- 241224/2045
Untrusted Pointer Dereferenc e CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the -3 3-4 4-5 5-6	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-SA72- 241224/2046 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handle is not validated by the service. CVE ID : CVE-2024-33039	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: sa'	7775p_firmwa	re			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA77- 241224/2047
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA77- 241224/2048
Integer Overflow or Wraparoun d CVSSv3 Scoring	02-Dec-2024 Scale 0-1	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https:// docs.qua lcomm.c om/pro duct/pu 6-7 7-8	0-QUA-SA77- 241224/2049 8-9 9-10

Dereferenc e02-Dec-20246.7Value as handle is not validated by handle is not validated by the service. CVE ID : CVE-2024-33039urces/se curitybu lletin.de cember- 2024- bulletin. html241224/205Product: sa8145p_firmwareMemory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu letin.de02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-330440-QUA-SA81 241224/205BufferMemory corruption when allocating and accessing an BufferMemory corruption when allocating and accessing an Uncest and the second constraints of the second constraints	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Pointer Dereferenc e02-Dec-20246.7Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039does.qua lcomm.c om/pro duct/pu blicreso ucces/se curitybu lletin./de cember- 2024- bulletin. httml0-QUA-SA77 241224/205Product: sa8145p_firmwareKemory corruption while COE ID : CVE-2024-33039https:// docs.qua lcomm.c om/pro duct/pu blicreso ucces/se curitybu lletin./de cember- 2024- bulletin. httmlo-QUA-SA77 241224/205Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso ucces/se curitybu lletin./de cember- 2024- bulletin. httmlBufferaMemory corruption when allocating and accessing an allocating and accessing an or sume blicreso ucres/se curitybu blicerso ucres/se curitybu blicerso ucres/se curitybu blicerso ucres/se curitybu blicerso ucres/se curitybu blicerso ucres/se curitybu blicerso ucres/se curitybu blicerso ucres/se curitybu blicerso ucres/se curitybu blicerso ucres/se curitybu blicerso ucres/se curitybu blicerso ucres/se curitybu blicerso ucres/se curitybu blicerso ucres/se curitybu blicerso ucres/se curitybu blicerso ucres/se curitybu blicerso ucres/se curitybu blicerso ucres/se curitybu blicerso ucres/se curitybu blice				this element is present.	urces/se curitybu lletin/de cember- 2024- bulletin.	
Affected Version(s): - Improper Validation of Array Index 02-Dec-2024 8.4 Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044 Index Memory corruption when allocating and accessing an allocating and accessing an locs.qua locs.qua COULA-SA81 O-QUA-SA81	Pointer Dereferenc	02-Dec-2024	6.7	PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	O-QUA-SA77- 241224/2050
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-SA81 0-QUA-SA81BufferMemory corruption when allocating and accessing an allocating and accessing an ocs.qua loommer0-QUA-SA81 0-QUA-SA81			re			
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-SA81 241224/205BufferMemory corruption when allocating and accessing an locs.qua0-QUA-SA81 0-QUA-SA81	Affected Ver	sion(s): -				
allocating and accessing an docs.qua	Validation of Array	02-Dec-2024	8.4	Configuring the SMR/S2CR register in Bypass mode.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	O-QUA-SA81- 241224/2051
		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu	0-QUA-SA81- 241224/2052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SA81- 241224/2053
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA81- 241224/2054
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	O-QUA-SA81- 241224/2055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- bulletin. html	
Product: sa	8150p_firmwa	re			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA81- 241224/2056
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA81- 241224/2057
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-SA81- 241224/2058

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
				bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA81- 241224/2059
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA81- 241224/2060
	8155p_firmwa	re			
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-SA81- 241224/2061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA81- 241224/2062
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA81- 241224/2063
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA81- 241224/2064

0-1

1-2

2-3

Page **921** of **1137**

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA81- 241224/2065
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA81- 241224/2066
Product: sa	8155_firmwar	e		·	
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA81- 241224/2067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA81- 241224/2068
	8195p_firmwa	re			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA81- 241224/2069
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA81- 241224/2070

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
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA81- 241224/2071
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA81- 241224/2072
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA81- 241224/2073
Buffer Over-read CVSSv3 Scoring	02-Dec-2024 Scale 0-1	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-SA81- 241224/2074 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: sa	8255p_firmwa	re			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA82- 241224/2075
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA82- 241224/2076
Integer Overflow or Wraparoun d CVSSv3 Scoring	02-Dec-2024 Scale 0-1	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater -3 3-4 4-5 5-6	https:// docs.qua lcomm.c om/pro duct/pu 6-7 7-8	0-QUA-SA82- 241224/2077 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html				
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA82- 241224/2078			
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA82- 241224/2079			
Product: sa8295p_firmware								
Affected Ver	sion(s): -			https://				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	docs.qua lcomm.c om/pro duct/pu blicreso	O-QUA-SA82- 241224/2080			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SA82- 241224/2081
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA82- 241224/2082
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	0-QUA-SA82- 241224/2083

Use After Free 02-Dec-2024 6.7 Memory corruption when multiple threads try to unregister the CVP buffer at the same time. https:// docs.qua com/ro duct/pu bilietin/de cember- 2024- bulletin/de 0-QUA-SA82- 241224/2084 Buffer Over-read 02-Dec-2024 6.1 Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. https:// docs.qua icomm.c om/pro duct/pu bilcreso urces/se curitybu 0-QUA-SA82- 2024- bulletin/de cember- 2024- bulletin/de cember- 2024- bulletin/de cember- 2024- bulletin/de cember- 2024- bulletin/de cember- 2024- bulletin/de cember- 2024- bulletin/de cember- 2024- bulletin/de cember- 2024- bulletin/de cember- 2024- bulletin/de cember- 2024- bulletin/de cember- 2024- bulletin/de cember- 2024- Product saB530p_firmware Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044 https:// docs.qua icomm.c om/pro duct/pu bilcreso curces/se curitybu lletin/de cember- 2024-	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free0.2 - Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053docs.qua locurtybu Differed curtybu Detrined curtybu Detrined LI224/20840QUA-SA82- 241224/2084Buffer Over-read0.2 - Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't vereived from the firmware. CVE ID : CVE-2024-33057https:// docs.qua locmm.c om/pro duct/pu blicreso Urces/se curtybu locures					bulletin.	
Buffer Over-readQ2-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-33037docs.qua curces/se 2024- bulletin. htmldocs.qua curces/se 241224/2085Product: sate-circle sate-c		02-Dec-2024	6.7	multiple threads try to unregister the CVP buffer at the same time.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	-
Affected Version(s): - Improper Validation of Array Index 02-Dec-2024 8.4 Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044 https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- 0-QUA-SA85- 241224/2086 CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10		02-Dec-2024	6.1	NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	-
Improper Validation of Array Index 02-Dec-2024 8.4 Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044 https:// docs.qua lcomm.c oduct/pu blicreso urces/se curitybu lletin/de c2024- 0-QUA-SA85- 241224/2086 CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Product: sa	8530p_firmwa	re			
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-0-QUA-SA85- 241224/2086CVSSv3 Scoring Scale0-11-22-33-44-55-66-77-88-99-10	Affected Ver	sion(s): -				
	Validation of Array	02-Dec-2024	8.4	Configuring the SMR/S2CR register in Bypass mode.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	-
			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
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA85- 241224/2087
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA85- 241224/2088
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA85- 241224/2089

 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	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA85- 241224/2090
	8540p_firmwa	re			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SA85- 241224/2091
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA85- 241224/2092

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA85- 241224/2093
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA85- 241224/2094
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA85- 241224/2095
	8620p_firmwa	re			
Affected Vers	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA86- 241224/2096
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA86- 241224/2097
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA86- 241224/2098
Untrusted Pointer Dereferenc e CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the -3 3-4 4-5 5-6	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-SA86- 241224/2099 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handle is not validated by the service. CVE ID : CVE-2024-33039	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: sa	8650p_firmwa	re			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA86- 241224/2100
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA86- 241224/2101
Integer Overflow or Wraparoun d CVSSv3 Scoring	02-Dec-2024 Scale 0-1	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https:// docs.qua lcomm.c om/pro duct/pu	0-QUA-SA86- 241224/2102 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA86- 241224/2103
	8770p_firmwa	re			
Affected Ver	sion(s): -			http://	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA87- 241224/2104
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	0-QUA-SA87- 241224/2105

			urces/se curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA87- 241224/2106
02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA87- 241224/2107
-	re		I	
sion(s): -				
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	O-QUA-SA87- 241224/2108
	02-Dec-2024 8775p_firmwa sion(s): -	02-Dec-2024 6.7 8775p_firmware sion(s): -	02-Dec-20247.5parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-3306302-Dec-20246.7Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-330398775p_firmwaresion(s): -02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode.	cember- 2024- bulletin. html02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin. html02-Dec-20246.7Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33063https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin. html8775p_firmwareMemory corruption when PAL client calls PAL service CVE ID : CVE-2024-33039https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin. html8775p_firmwareMemory corruption whei Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro

Weakness	Publish Date	CVSSv3	Description & CV	/E ID	Patch	NCIIPC ID
					curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption allocating and acces entry in an SMEM pa continuously. CVE ID : CVE-2024	sing an artition	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA87- 241224/2109
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE w beacon with commo length of the ML IE g than the ML IE insid this element is press CVE ID : CVE-2024	rhen a on info greater le which ent.	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA87- 241224/2110
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption PAL client calls PAL APIs by passing a ra value as handle and handle is not validat the service. CVE ID : CVE-2024	service indom the ted by	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-SA87- 241224/2111
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6	5-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Product: sa	9000p_firmwa	re			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SA90- 241224/2112
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA90- 241224/2113
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-SA90- 241224/2114

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SA90- 241224/2115
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA90- 241224/2116
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SA90- 241224/2117

 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	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SA90- 241224/2118
	8180x_firmwa	re			
Affected Ver	sion(s): -			h	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SC81- 241224/2119
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SC81- 241224/2120

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
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SC81- 241224/2121
-	8380xp_firmw	are			
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SC83- 241224/2122
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SC83- 241224/2123

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SC83- 241224/2124
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SC83- 241224/2125
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SC83- 241224/2126
Improper Restriction of Operations CVSSv3 Scoring	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-SC83- 241224/2127 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			target diagnostic information. CVE ID : CVE-2024-43053	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: sd	460_firmware				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SD46- 241224/2128
Product: sd	660_firmware				
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SD66- 241224/2129
Product: sd	662_firmware				
	. ()				
Affected Ver	rsion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SD66- 241224/2130
Product: sd	670_firmware				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SD67- 241224/2131
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SD67- 241224/2132
Product: sd	675_firmware				
CVSSv3 Scoring		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10
*stands for all v	versions		Page 9/2 of 1127		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SD67- 241224/2133
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SD67- 241224/2134
Product: sd	730_firmware				
Affected Vers	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SD73- 241224/2135
CVSSv3 Scoring *stands for all v		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 Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SD73- 241224/2136
Product: sd	835_firmware			1	
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SD83- 241224/2137
Product: sd	855_firmware				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-SD85- 241224/2138

 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
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SD85- 241224/2139
	865_5g_firmwa	are			
Affected Ver	sion(s): -			I	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SD86- 241224/2140
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-SD86- 241224/2141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SD86- 241224/2142
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SD86- 241224/2143
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SD86- 241224/2144

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

 *stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SD86- 241224/2145
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SD86- 241224/2146
Product: sd	888_firmware				
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SD88- 241224/2147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SD88- 241224/2148
	m429w_firmw	are			
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SDM4- 241224/2149
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SDM4- 241224/2150

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SDM4- 241224/2151
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SDM4- 241224/2152
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SDM4- 241224/2153
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input.	https:// docs.qua lcomm.c om/pro 6-7 7-8	O-QUA-SDM4- 241224/2154 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			CVE ID : CVE-2024-43052	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SDM4- 241224/2155		
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SDM4- 241224/2156		
Product: sdx20m_firmware							
Affected Vers	sion(s): -			1			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro duct/pu	O-QUA-SDX2- 241224/2157		
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-2024-33056	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
	x55_firmware				
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SDX5- 241224/2158
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SDX5- 241224/2159
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver.	https:// docs.qua lcomm.c om/pro duct/pu blicreso	0-QUA-SDX5- 241224/2160

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

						CVE ID					PC ID
			CV	E ID : C	VE-202	4-43050	0 1 0 2 1 2	curit	ŀ- etin.		
Improper Input Validation	02-Dec-2024	7.8	pro wi	th invali	API cal d input.	n while ls to NPU 4-43052	J 1 1 1 1 1 1 1 2 1 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1	com om/j duct olicr urce curit	.qua m.c pro /pu eso s/se ybu h/de per- t- etin.	0-QUA- 241224	
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	pai car var alle ane to me	d parsin huge alle emory ac	nsor pac ver, use used wl nemory g which ocation ccess.	kets in r-space	el u d 1 2 2 3 4 3 2 3 5 4 3 2 3 5 4 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	com om/j duct olicr urce curit	.qua m.c pro /pu eso s/se ybu h/de per- t- etin.	0-QUA- 241224	
Use After Free	02-Dec-2024	6.7	mu un the	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053				com om/j duct olicr urce curit	.qua m.c pro /pu eso s/se ybu n/de	0-QUA- 241224	

Buffer Over-read02-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message to NPU driver as the driver doesn't validate the IPC message to NPU blicresso urces/se curitybu letin/de0-QUA-SDX5- 241224/2164Product: sdx57m_firmwareKemory corruption while COFiguring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33034https:// does.qua letin/de0-QUA-SDX5- 241224/2164Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua loc	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read02-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-33037docs.qua locmber- 2024- bulletin. httmO-QUA-SDX5- 241224/2164Product: sdx57m_firmwareImage (CVE ID : CVE-2024-33037)O-QUA-SDX5- (CVE ID : CVE-2024-33037)O-QUA-SDX5- 241224/2164Improper Validation of Array Index02-Dec-20248.4Memory corruption while configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso curitybu letin/de cember- 2024- bulletin. httmlO-QUA-SDX5- 241224/2165Buffer Over-read02-Dec-20248.4Memory corruption wheil entry in an SMEM partition continuously. CVE ID : CVE-2024-33056O-QUA-SDX5- 241224/2165					bulletin.	
Affected Version(s): -Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu letin/de0-QUA-SDX5- 241224/2165Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu		02-Dec-2024	6.1	NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	-
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044 https:// docs.qua lcomm.c ources/se curitybu lletin/de cember- 2024- bulletin. httml0-QUA-SDX5- 241224/2165Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056 https:// docs.qua lcomm.c0-QUA-SDX5- 241224/2165	-		e			
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044 docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-SDX5- 241224/2165Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	Affected Ver	sion(s): -		r		
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.docs.qua lcomm.c om/pro duct/pu blicreso urces/se0-QUA-SDX5- 241224/2166	Validation of Array	02-Dec-2024	8.4	Configuring the SMR/S2CR register in Bypass mode.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	e
cember- 2024-		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	•

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
				bulletin. html					
Product: sd	x61_firmware								
Affected Version(s): -									
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SDX6- 241224/2167				
Product: sd	x65m_firmwar	·e							
Affected Ver	sion(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SDX6- 241224/2168				
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	O-QUA-SDX6- 241224/2169				

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
				cember- 2024- bulletin. html		
Product: sd	x71m_firmwar	e				
Affected Ver	sion(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SDX7- 241224/2170	
Product: sd	_455_firmware	•				
Affected Ver	sion(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SD_4- 241224/2171	
Product: sd_675_firmware Affected Version(s): -						
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu	O-QUA-SD_6- 241224/2172	
CVSSv3 Scoring stands for all v		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 <mark>9-10</mark>	

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SD_6- 241224/2173
_8cx_firmware				
sion(s): -			1	
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SD_8- 241224/2174
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	O-QUA-SD_8- 241224/2175
	02-Dec-2024 02-Dec-2024 02-Dec-2024	o o	o2-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056o2-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044o2-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044o2-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httml02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httml02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httml02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso curitybu lletin/de cember- 2024- bulletin. httml02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c com/pro duct/pu

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
				urces/se curitybu lletin/de cember- 2024- bulletin. html			
Product: sd	8_gen1_5g_fir	mware		1			
Affected Ver	sion(s): -						
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SD_8- 241224/2176		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SD_8- 241224/2177		
Product: sg4150p_firmware							
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro	O-QUA-SG41- 241224/2178		
CVSSv3 Scoring *stands for all v		1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

-SG41- 4/2179
-SG82- 4/2180
-SG82- 4/2181

				blicreso		
				urces/se curitybu lletin/de cember- 2024- bulletin. html		
Integer Overflow or 0 Wraparoun d)2-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SG82- 241224/2182	
Product: sm42	125_firmwar	е				
Affected Version	on(s): -					
Buffer Over-read 0	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SM41- 241224/2183	
Product: sm4635_firmware						
Affected Versio	on(s): -					
Buffer Over-read)2-Dec-2024	8.4	Memory corruption when allocating and accessing an	https:// docs.qua lcomm.c	0-QUA-SM46- 241224/2184	
CVSSv3 Scoring Sc	cale 0-1	1-2 2	- 3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Buffer Overflow02-Dec-20247.8Invoke of of nearborn ATT call.thread of in ATT call.t	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack- based Buffer Overflow02-Dec-20247.8Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048docs.qua lcomm.c om/pro duct/pu blicreso ucces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-SM4 241224/218Product: sm6250p_firmwareAffected Version(s): -Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlBuffer02-Dec-20248.4Memory corruption when allocating and accessing an allocating and accessing anhttps:// docs.qua o-QUA-SM6				continuously.	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	
Affected Version(s): -Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-SM6 241224/218Buffer02-Dec-20248.4Memory corruption when allocating and accessing anhttps:// docs.qua 	based Buffer	02-Dec-2024	7.8	invalid input is passed to invoke GPU Headroom API call.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	0-QUA-SM46- 241224/2185
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-SM6 241224/218Buffer02-Dec-20248.4Memory corruption when allocating and accessing anhttps:// docs.qua 0-QUA-SM6			are			
Improper Validation of Array Index02-Dec-20248.4Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de 2024- bulletin. html0-QUA-SM6 241224/218Buffer02-Dec-20248.4Memory corruption when allocating and accessing an allocating and accessing anhttps:// docs.qua	Affected Ver	sion(s): -			1	
Buffer 02-Dec-2024 84 allocating and accessing an docs.qua 0-QUA-SM6	Validation of Array	02-Dec-2024	8.4	Configuring the SMR/S2CR register in Bypass mode.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	O-QUA-SM62- 241224/2186
		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c	0-QUA-SM62- 241224/2187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			CVE ID : CVE-2024-33056	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html			
Product: sm	16250_firmwar	е					
Affected Vers	sion(s): -						
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SM62- 241224/2188		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SM62- 241224/2189		
Product: sm6370_firmware							
Affected Version(s): -							
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https:// docs.qua	0-QUA-SM63- 241224/2190		
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: sm	17250p_firmwa	are		I	
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SM72- 241224/2191
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SM72- 241224/2192
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to	https:// docs.qua lcomm.c	0-QUA-SM72- 241224/2193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
-	17315_firmwa1	'e			
Affected Vers	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SM73- 241224/2194
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SM73- 241224/2195
Product: sm	7325p_firmwa	are		•	
Affected Vers	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SM73- 241224/2196
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SM73- 241224/2197
Product: sm	18550p_firmwa	are			
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SM85- 241224/2198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SM85- 241224/2199	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SM85- 241224/2200	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SM85- 241224/2201	
Product: sm8635_firmware						
Affected Ver	sion(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SM86- 241224/2202
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SM86- 241224/2203
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SM86- 241224/2204
Integer Overflow or CVSSv3 Scoring	02-Dec-2024	7.5	Transient DOS whileparsing the ML IE when abeacon with common infolength of the ML IE greater-33-44-55-6	https:// docs.qua lcomm.c om/pro 6-7 7-8	O-QUA-SM86- 241224/2205 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparoun d			than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
	18750p_firmwa	are			
Affected Ver	sion(s): -			1	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SM87- 241224/2206
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SM87- 241224/2207
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu	0-QUA-SM87- 241224/2208

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SM87- 241224/2209
	18750_firmwai	e			
Affected Ver Buffer Over-read	sion(s): - 02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SM87- 241224/2210
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso	0-QUA-SM87- 241224/2211

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			urces/se curitybu lletin/de cember- 2024- bulletin. html					
02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SM87- 241224/2212				
02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SM87- 241224/2213				
Product: smart_audio_200_platform_firmware								
sion(s): -		Γ						
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	O-QUA-SMAR- 241224/2214				
	02-Dec-2024 02-Dec-2024 02-Dec-2024	02-Dec-2024 7.8 02-Dec-2024 7.5 02-Dec-2024 7.5	O2-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-4305202-Dec-20247.8Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063o2-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua lcomm.c om/pro duct/pu blicreso02-Dec-20247.8Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063https:// docs.qua lcomm.c om/pro duct/pu blicreso02-Dec-20248.4Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua lcomm.c om/pro duct/pu blicreso02-Dec-20248.4Memory corruption while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063https:// docs.qua lcomm.c om/pro duct/pu blicreso02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33066https:// docs.qua locm.c om/pro				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
				curitybu lletin/de cember- 2024- bulletin. html					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SMAR- 241224/2215				
Product: sm	Product: smart_audio_400_platform_firmware								
Affected Ver	sion(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SMAR- 241224/2216				
Product: snapdragon_1100_wearable_platform_firmware									
Affected Version(s): -									
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu	O-QUA-SNAP- 241224/2217				
CVSSv3 Scoring *stands for all v		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			
				blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html				
		0_wearab	le_platform_firmware					
Affected Ver	sion(s): -			1				
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlo-QUA-SNAP- 241224/2218								
Product: sn Affected Ver	apdragon_208	_processo	or_firmware					
Allected ver	sion(s): -			http://				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2219			
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input.	https:// docs.qua lcomm.c	O-QUA-SNAP- 241224/2220			

Improper Improper Improper Improper Nalidation02-Dec-20248.4Remory corruption when allocating and accessing an continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso uccessing an entry im a SMEM partition ontinuously. CVE ID : CVE-2024-330560-QUA-SNAP- 241224/2221Improper Ipput Validation02-Dec-20247.8Memory corruption when allocating and accessing an ontinuously. CVE ID : CVE-2024-330560-QUA-SNAP- 241224/2221Improper Ipput Validation02-Dec-20247.8Memory corruption when allocating and accessing an ontinuously. CVE ID : CVE-2024-330560-QUA-SNAP- 241224/2221Improper Ipput Validation02-Dec-20247.8Memory corruption wheile processing API calls to NPU with invalid input. CVE ID : CVE-2024-430520-QUA-SNAP- 241224/2222Product: smature. Z024- builetin. html0-QUA-SNAP- 241224/2222Product: smature. Z024- builetin. html0-QUA-SNAP- 241224/2222	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Version(s): -Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso curitybu lletin/de cember- 2024- bulletin. html-QUA-SNAP- 241224/2221Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua letin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se				CVE ID : CVE-2024-43052	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.				
Buffer Over-read02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. htmlo-QUA-SNAP- 241224/2221Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU 	Product: sn	apdragon_210	_processo	or_firmware					
Buffer Over-read0.2-Dec-20248.4Remory corruption when entry in an SMEM partition continuously. CVE ID : CVE-2024-33056docs.qua com/pro ucres/se uc	Affected Ver	sion(s): -							
Improper Imput Validation02-Dec-20247.8Amenory corruption while processing API calls to NPU Att invalid input. CVE ID : CVE-2024-43052docs.qua Icomuc duct/pu blicresso (curitybu) Icember- 2024- builetin, builetin, totalProduct: superstretsuperstretsuperstret		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•			
	Input	02-Dec-2024	7.8	processing API calls to NPU with invalid input.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•			
Affected Version(s): -	Product: sn								
	Affected Ver	sion(s): -							

Buffer Over-read 02-Dec-2024 8.4 Memory corruption when allocating and accessing an entry in an SMEM partition continuously. 0-QUA-SNAP- 241224/2223 Improper Input Validation 02-Dec-2024 7.8 Memory corruption while processing API calls to NPU with invalid input. https:// docs.qua icember- 2024- bulletin, html 0-QUA-SNAP- 241224/2223 Improper Input Validation 02-Dec-2024 7.8 Memory corruption while processing API calls to NPU with invalid input. https:// docs.qua icember- 2024- bulletin, html 0-QUA-SNAP- 241224/2224 Product: snapdragon_425_mobile_platform_firmware https:// docs.qua icember- 2024- bulletin, html 0-QUA-SNAP- 241224/2224 Improper Input Validation 02-Dec-2024 7.8 Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052 https:// docs.qua icember- 2024- bulletin, html Improper Input Validation 02-Dec-2024 7.8 Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052 https:// docs.qua icember- 2024- bulletin, html Product: snapdragon_427_mobile_platform_firmware https:// docs.qua icember- 2024- bulletin, html 0-QUI-SNAP- 241224/2225	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu letin/de cember- 2024- builetin. html0-QUA-SNAP- 241224/2224Product: smaptragon_425-mobile verson 2024- builetin. htmlMemory corruption while processing API calls to NPU builetin. htmlhttps:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu letin/de cember- 2024- builetin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se urces		02-Dec-2024	8.4	allocating and accessing an entry in an SMEM partition continuously.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•
Affected Version(s): - https://docs.qua Improper 02-Dec-2024 7.8 Memory corruption while https://docs.qua Validation 02-Dec-2024 7.8 Memory corruption while om/pro Validation 02-Dec-2024 7.8 Memory corruption while om/pro Validation 02-Dec-2024 7.8 Memory corruption while om/pro Validation 02-Dec-2024 7.8 Validation O-QUA-SNAP- CVE ID : CVE-2024-43052 Validation O-QUA-SNAP- Product: snaper_appr_427_mobile_paper_appr_44 Validation Validation Validation CVSSv3 Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Input	02-Dec-2024	7.8	processing API calls to NPU with invalid input.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	-
Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua lcom.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-SNAP- 241224/2225Product: superson_427_mobile_ztom_firmwareCVSSv3 Scoring Scale0-11-22-33-44-55-66-77-88-99-10	Product: sn	apdragon_425	_mobile_p	olatform_firmware		
Improper Input Validation02-Dec-20247.87.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052docs.qua lcom.c om/pro duct/pu blicreso ucces/se Curitybu lletin/de 	Affected Ver	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	Input	02-Dec-2024	7.8	processing API calls to NPU with invalid input.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•
	Product: sn	apdragon_427	_mobile_p	blatform_firmware	I	
			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	Affected Version(s): -							
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2226			
		_mobile_p	olatform_firmware					
Affected Vers	sion(s): -			1				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2227			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2228			
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10			

				https://	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2229
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2230
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2231
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input.	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-SNAP- 241224/2232 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			CVE ID : CVE-2024-43052	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2233				
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2234				
	Product: snapdragon_430_mobile_platform_firmware								
Affected Vers	sion(s): -			-					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu	0-QUA-SNAP- 241224/2235				
CVSSv3 Scoring	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html				
	• •	_mobile_p	olatform_firmware					
Affected Ver	sion(s): -			T				
Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-SNAP- 241224/2236								
Product: sn	apdragon_439	_mobile_p	olatform_firmware	I				
Affected Ver	sion(s): -							
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2237			
Product: sn	apdragon_460	_mobile_p	olatform_firmware	I	I			
Affected Ver	sion(s): -							

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2238
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2239
Product: sn	apdragon_480	\+_5g_mo	bile_platform_firmware		
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2241		
Product: sn	apdragon_480	_5g_mobi	le_platform_firmware				
Affected Ver	sion(s): -						
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2242		
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2243		
Product: sn	Product: snapdragon_4_gen_1_mobile_platform_firmware						
CVSSv3 Scoring		1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		
*stands for all v	rersions		Dage 990 of 1127				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2244
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2245
Product: sna	apdragon_4_ge	en_2_mob	ile_platform_firmware		
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2246
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		Descrip	tion & C	VE ID		Patch	NCII	PC ID
Product: snapdragon_630_mobile_platform_firmware										
Affected Ver	sion(s): -									
Buffer Over-read	02-Dec-2024	8.4	alloca entry contin	iting a in an nuous	nd acce SMEM ly.	n when essing an partition 4-33056	dc lcc or du bl ur cu lle ce 20 bu	tps:// ocs.qua omm.c n/pro ict/pu icreso cces/se critybu etin/de mber- 024- illetin. ml	0-QUA- 241224	
Product: sn	apdragon_636	_mobile_j	platfor	m_fir	mware	!				
Affected Ver	sion(s): -									
Buffer Over-read	02-Dec-2024	8.4	alloca entry contin	iting a in an nuous	nd acce SMEM ly.	n when essing an partition 4-33056	dc lcc or du bl ur cu lle ce 20 bu	tps:// ocs.qua omm.c n/pro act/pu icreso cces/se aritybu etin/de mber- 024- alletin. ml	0-QUA- 241224	
Product: sn	apdragon_660	_mobile_j	platfor	m_fir	mware					
Affected Ver	sion(s): -									
Buffer Over-read	02-Dec-2024	8.4	alloca entry contin	iting a in an nuous	nd acce SMEM ly.	n when essing an partition 4-33056	do lco or du bl ur cu	tps:// ocs.qua omm.c n/pro nct/pu icreso cces/se ritybu etin/de	0-QUA- 241224	
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
				cember- 2024- bulletin. html	
Product: sn	apdragon_662	_mobile_p	olatform_firmware		
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2250
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2251
Product: sn	apdragon_665	_mobile_p	olatform_firmware		I
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	0-QUA-SNAP- 241224/2252

CVSSv3 Scoring Scale 3-4 0-1 1-2 2-3 *stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
				curitybu lletin/de cember- 2024- bulletin. html			
		_mobile_p	olatform_firmware				
Affected Ver	sion(s): -		1	1			
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2253		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2254		
Product: sna	Product: snapdragon_675_mobile_platform_firmware						
Affected Version(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu	O-QUA-SNAP- 241224/2255		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2256
		_mobile_p	olatform_firmware		
Affected Ver Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2257
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	O-QUA-SNAP- 241224/2258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sn	andragon 680	4g mohi	le_platform_firmware	urces/se curitybu lletin/de cember- 2024- bulletin. html	
Affected Ver		- 19_111001			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2259
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2260
		_4g_mobi	le_platform_firmware		
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro	0-QUA-SNAP- 241224/2261
CVSSv3 Scoring		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-2024-33056	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2262
Product: sn	apdragon_690	_5g_mobi	le_platform_firmware		
Affected Ver	sion(s): -			I	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2263
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro duct/pu	O-QUA-SNAP- 241224/2264

4-5

5-6

6-7

7-8

8-9

9-10

3-4

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2265
		_5g_mobi	le_platform_firmware		
Affected Ver Buffer Over-read	sion(s): - 02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2266
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso	O-QUA-SNAP- 241224/2267

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sna	apdragon 710	mobile r	platform_firmware	urces/se curitybu lletin/de cember- 2024- bulletin. html	
Affected Vers					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2268
Product: sna	apdragon_712	_mobile_p	blatform_firmware		
Affected Vers	sion(s): -			1	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2269
Product: sna	apdragon_720	g_mobile_	_platform_firmware	I	I
Affected Vers	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2270
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2271
Product: sn	apdragon_730	g_mobile	platform_firmware		
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2273		
Product: sn	apdragon_730	_mobile_p	olatform_firmware				
Affected Ver	sion(s): -						
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2274		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2275		
Product: sn	Product: snapdragon_732g_mobile_platform_firmware						
CVSSv3 Scoring	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10		
*stands for all v	versions		Page 991 of 1127				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): -	L			
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2276
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2277
Product: sna	apdragon_750	g_5g_mob	oile_platform_firmware	<u> </u>	
Affected Vers	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2278
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 Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2279
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2280
		g_5g_mob	ile_platform_firmware	·	
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2282
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2283
Product: sn	apdragon_765	_5g_mobi	le_platform_firmware		
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2285
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2286
		g_5g_mob	oile_platform_firmware		
Affected Ver	sion(s): -		I	1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2288
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2289
		g\+_5g_m	obile_platform_firmware		
Affected Ver	sion(s): -		I	1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2291			
Product: sn	apdragon_778	g_5g_mob	oile_platform_firmware					
Affected Ver	sion(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2292			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2293			
Product: sn	Product: snapdragon_780g_5g_mobile_platform_firmware							
CVSSv3 Scoring		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10			
*stands for all v	versions		Dage 997 of 1127					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): -	L			
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2294
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2295
Product: sna	apdragon_782	g_mobile_	platform_firmware		
Affected Vers	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2296
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 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 Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2297
		⊦_gen_3_c	ompute_firmware		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2298
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2299

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2300
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2301
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2302
		ompute_j	platform_firmware		
Affected Vers	sion(s): -				

0-1

1-2

5-6 6-7 8-9

9-10

7-8

*stands for all versions

4-5

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2303
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2304
Product: sn	apdragon_7c_g	gen_2_con	npute_platform_firmware		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2306
Product: sn	apdragon_820	_automot	ive_platform_firmware		
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2307
Product: sn	apdragon_835	_mobile_p	oc_platform_firmware		
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-SNAP- 241224/2308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
				bulletin. html						
Product: sn	Product: snapdragon_845_mobile_platform_firmware									
Affected Ver	sion(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2309					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2310					
Product: sn	apdragon_850	_mobile_c	compute_platform_firmware							
Affected Ver	sion(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	0-QUA-SNAP- 241224/2311					

4-5

5-6

6-7

7-8

8-9

9-10

3-4

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2312
	apdragon_855	\+_firmw	are		
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2313
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	O-QUA-SNAP- 241224/2314

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- bulletin. html	
Product: sn	apdragon_855	_mobile_p	olatform_firmware		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2315
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2316
Product: sn	apdragon_860	_mobile_p	olatform_firmware		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	0-QUA-SNAP- 241224/2317

2-3

3-4

4-5

5-6

6-7

7-8

8-9

9-10

CVSSv3 Scoring Scale *stands for all versions

0-1

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2318
		\+_5g_mo	bile_platform_firmware		
Affected Ver	sion(s): -			-	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2319
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	O-QUA-SNAP- 241224/2320

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2321
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2322
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2324
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2325
Product: sn	apdragon_865	_5g_mobi	le_platform_firmware	•	
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2327
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2328
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2329
Use After Free CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as	https:// docs.qua lcomm.c om/pro 6-7 7-8	O-QUA-SNAP- 241224/2330 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html				
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2331			
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2332			
		_5g_mobi	le_platform_firmware					
Affected Ver	Affected Version(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu	O-QUA-SNAP- 241224/2333			
CVSSv3 Scoring	Scale 0-1	1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2334
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2335
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access.	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	O-QUA-SNAP- 241224/2336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33036	cember- 2024- bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2337
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2338
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Product: sn	Product: snapdragon_888\+_5g_mobile_platform_firmware								
Affected Ver	Affected Version(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2340				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2341				
		_5g_mobi	le_platform_firmware						
Affected Ver	sion(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-SNAP- 241224/2342				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2343
		compute	_platform_firmware		
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2344
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-SNAP- 241224/2345

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2346
		gen_2_5g	_compute_platform_firmwar	е	
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2347
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-SNAP- 241224/2348

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2349
		gen_3_co	mpute_platform_firmware		
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2350
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-SNAP- 241224/2351

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2352
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2353
		ompute_j	platform_firmware		
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-SNAP- 241224/2354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2355
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2356
		_gen_1_m	obile_platform_firmware		
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-SNAP- 241224/2357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Product: sn	apdragon_8\+	_gen_2_m	obile_platform_firmware	·	
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2358
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2359
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-SNAP- 241224/2360

4-5

5-6

6-7

7-8

8-9

9-10

3-4

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2361
Product: sn	apdragon_8_ge	en_1_mob	ile_platform_firmware		
Affected Ver	sion(s): -			-	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2362
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-SNAP- 241224/2363

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2364
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2365
		en_2_mob	ile_platform_firmware		
Affected Ver	sion(s): -			-	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-SNAP- 241224/2366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2367
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2368
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2369
Product: sna			-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 Ver	Affected Version(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2370			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2371			
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2372			

 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
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2373
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2374
		gen_1_pla	atform_firmware	·	
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2375

 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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2376
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2377
Product: sna	apdragon_auto	o_4g_mod	em_firmware		
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2379			
Product: sn	apdragon_auto	o_5g_mod	em-rf_firmware					
Affected Ver	sion(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2380			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2381			
Product: sn	Product: snapdragon_auto_5g_modem-rf_gen_2_firmware							
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 v	versions		Daga 1036 of 1137					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2382		
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2383		
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2384		
Product: snapdragon_w5\+_gen_1_wearable_platform_firmware							
Affected Version(s): -							
CVSSv3 Scoring *stands for all v		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 Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2385
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2386
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2387
Use After Free CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as	https:// docs.qua lcomm.c om/pro 6-7 7-8	O-QUA-SNAP- 241224/2388 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2389
		r_1300_p	latform_firmware		
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2390
		r_2100_p	latform_firmware		
Affected Ver	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2391
Product: sn	apdragon_wea	r_2500_p	latform_firmware	<u> </u>	
Affected Ver	sion(s): -				
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2392
	• •	r_3100_p	latform_firmware		
Affected Ver	sion(s): -				
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-SNAP- 241224/2393

 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					
				bulletin. html						
Product: sn	Product: snapdragon_wear_4100\+_platform_firmware									
Affected Ver	sion(s): -									
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2394					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2395					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-SNAP- 241224/2396					

 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				
				bulletin. html					
Product: sn	Product: snapdragon_x12_lte_modem_firmware								
Affected Ver	sion(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2397				
Product: sn	apdragon_x20	_lte_mode	em_firmware						
Affected Ver	sion(s): -								
Buffer Over-read	02-Dec-2024		Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2398				
	apdragon_x24	_lte_mode	em_firmware						
Affected Ver	sion(s): -			1-					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	O-QUA-SNAP- 241224/2399				
CVSSv3 Scoring *stands for all v		1-2 2	- <mark>3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2400
Product: sn	apdragon_x35	_5g_mode	m-rf_system_firmware		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2401
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	0-QUA-SNAP- 241224/2402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
		_5g_mode	em-rf_system_firmware		
Affected Ver Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2403
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2404
Product: sn	apdragon_x55	_5g_mode	em-rf_system_firmware		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso	O-QUA-SNAP- 241224/2405

 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	Descrij	otion & C	VE ID	Pa	tch	NCIIF	PC ID
						curi	4- etin.		
Buffer Over-read	02-Dec-2024	8.4	Memory co allocating a entry in an continuous CVE ID : CV	and acce SMEM j sly.	essing an partition	lcon om/ duct blict urce curi	s.qua nm.c pro t/pu reso es/se tybu n/de ber- 4- etin.	0-QUA- 241224	
Improper Input Validation	02-Dec-2024	7.8	Memory cc processing with invali CVE ID : C	API call d input.	s to NPU	lcon om/ duct blict urce curi	s.qua nm.c pro t/pu reso es/se tybu n/de ber- 4- etin.	0-QUA- 241224	
Use of Out- of-range Pointer Offset CVSSv3 Scoring	02-Dec-2024 Scale 0-1	6.7	Memory co parsing ser camera dri variable is allocating r and parsin to huge allo memory ac CVE ID : CV	nsor pac ver, use used wh nemory g which ocation o ccess.	kets in r-space nile in kerne can lead or invalid	lcon om/ duct blict urce curi	s.qua nm.c pro c/pu reso es/se tybu n/de	0-QUA- 241224	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2409
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2410
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2411

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Product: sn	Product: snapdragon_x5_lte_modem_firmware								
Affected Ver	Affected Version(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2412				
		_5g_mode	em-rf_system_firmware						
Affected Ver	sion(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2413				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-SNAP- 241224/2414				

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
				bulletin. html					
Product: snapdragon_x65_5g_modem-rf_system_firmware									
Affected Ver	Affected Version(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2415				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2416				
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-SNAP- 241224/2417				

Page 1038 of 1137

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
				bulletin. html					
Product: sn	Product: snapdragon_x70_modem-rf_system_firmware								
Affected Ver	sion(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2418				
Product: sn	apdragon_x72	_5g_mode	em-rf_system_firmware						
Affected Ver	sion(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2419				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	0-QUA-SNAP- 241224/2420				

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2421
Product: sn	apdragon_x75	_5g_mode	m-rf_system_firmware	·	
Affected Ver	sion(s): -			-	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2422
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	O-QUA-SNAP- 241224/2423

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2424
Product: sn	apdragon_xr1_	platform	_firmware		
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2425
Product: sn	apdragon_xr2	+_gen_1_	platform_firmware		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	0-QUA-SNAP- 241224/2426

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2427
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SNAP- 241224/2428
Product: sn	apdragon_xr2_	5g_platfo	orm_firmware		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	O-QUA-SNAP- 241224/2429
CVSSv3 Scoring		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10
*stands for all v	/ersions		Dage 10/12 of 1127		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2430
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2431
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2433
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2434
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SNAP- 241224/2435
	v1h_firmware				
Affected Ver	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SRV1- 241224/2436
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SRV1- 241224/2437
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SRV1- 241224/2438
Untrusted Pointer Dereferenc e CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the -3 3-4 4-5 5-6	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-SRV1- 241224/2439 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handle is not validated by the service. CVE ID : CVE-2024-33039	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
	v1l_firmware				
Affected Vers	sion(s): -			https://	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SRV1- 241224/2440
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SRV1- 241224/2441
	v1m_firmware			1	
Affected Vers	sion(s): -				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SRV1- 241224/2442
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SRV1- 241224/2443
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SRV1- 241224/2444
Untrusted Pointer Dereferenc e CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the -3 3-4 4-5 5-6	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-SRV1- 241224/2445 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handle is not validated by the service. CVE ID : CVE-2024-33039	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: ssg	g2115p_firmwa	are			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SSG2- 241224/2446
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SSG2- 241224/2447
Integer Overflow or Wraparoun d CVSSv3 Scoring	02-Dec-2024 Scale 0-1	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https:// docs.qua lcomm.c om/pro duct/pu	0-QUA-SSG2- 241224/2448 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
,	g2125p_firmwa	are			
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SSG2- 241224/2449
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SSG2- 241224/2450
Integer Overflow or Wraparoun d	02-Dec-2024 Scale 0-1	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	https:// docs.qua lcomm.c om/pro duct/pu blicreso	0-QUA-SSG2- 241224/2451 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33063	urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: sw	5100p_firmwa	ire			
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SW51- 241224/2452
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SW51- 241224/2453
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service.	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	O-QUA-SW51- 241224/2454

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		CVE ID : CVE-2024-33039	curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SW51- 241224/2455
02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SW51- 241224/2456
	е			
sion(s): -				
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	0-QUA-SW51- 241224/2457
	02-Dec-2024 02-Dec-2024 02-Dec-2024	02-Dec-2024 6.7 02-Dec-2024 6.7 02-Dec-2024 6.1	O2-Dec-20246.7Wemory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-3304002-Dec-20246.1Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-330375100_firmware02-Dec-20248.402-Dec-20248.4	O2-Dec-20246.7CVE ID : CVE-2024-33039curitybu lletin/de cember- 2024- bulletin. html02-Dec-20246.7Memory corruption while invoking redundant release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html02-Dec-20246.7Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-33037https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httml02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se urces/se

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SW51- 241224/2458
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SW51- 241224/2459
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-SW51- 241224/2460

0-1

1-2

Page **1052** of **1137**

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SW51- 241224/2461
	r1120_firmwa	re			
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SXR1- 241224/2462
Product: sx	r1230p_firmwa	are			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	O-QUA-SXR1- 241224/2463

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SXR1- 241224/2464
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SXR1- 241224/2465
	r2130_firmwa	re			
Affected Vers	sion(s): -			between 11	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	O-QUA-SXR2- 241224/2466
CVSSv3 Scoring *stands for all v		1-2 2	<mark>-3</mark> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SXR2- 241224/2467
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SXR2- 241224/2468
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SXR2- 241224/2469

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SXR2- 241224/2470
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SXR2- 241224/2471
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SXR2- 241224/2472
	r2230p_firmwa	are			
Affected Vers	sion(s): -				

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SXR2- 241224/2473
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SXR2- 241224/2474
Product: sx	r2250p_firmwa	are			
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-SXR2- 241224/2475

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-SXR2- 241224/2476
Product: tal	ynplus_firmwa	are			
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-TALY- 241224/2477
		ion_vc1_p	latform_firmware		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-VIDE- 241224/2478

 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
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-VIDE- 241224/2479
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-VIDE- 241224/2480
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-VIDE- 241224/2481

 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	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-VIDE- 241224/2482
		ion_vc3_p	latform_firmware		
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-VIDE- 241224/2483
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-VIDE- 241224/2484

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-VIDE- 241224/2485
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-VIDE- 241224/2486
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-VIDE- 241224/2487
Use After Free CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https:// docs.qua lcomm.c om/pro 6-7 7-8	O-QUA-VIDE- 241224/2488 8-9 9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33053	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-VIDE- 241224/2489
Product: via	deo_collaborat	ion_vc5_p	latform_firmware	I	
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-VIDE- 241224/2490
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https:// docs.qua lcomm.c om/pro duct/pu	O-QUA-VIDE- 241224/2491

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			CVE ID : CVE-2024-33056	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html			
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-VIDE- 241224/2492		
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-VIDE- 241224/2493		
Product: vision_intelligence_300_platform_firmware							
Affected Vers	sion(s): -			https://			
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	docs.qua lcomm.c om/pro duct/pu blicreso	0-QUA-VISI- 241224/2494		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-VISI- 241224/2495
		ce_400_pl	atform_firmware		
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-VISI- 241224/2496
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	0-QUA-VISI- 241224/2497

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-VISI- 241224/2498
02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-VISI- 241224/2499
	ire			
sion(s): -				
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	O-QUA-WCD9- 241224/2500
	02-Dec-2024 02-Dec-2024 02-Dec-2024	02-Dec-2024 7.8 02-Dec-2024 7.5 02-Dec-2024 7.5	O2-Dec-20247.8Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-4304802-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063cd9306_firmwarecolor_2-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	O2-Dec-2024A.B.Memory corruption when invalid input is passed to invoke GPU Headroom API call.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httm02-Dec-20247.8Memory corruption when invalid input is passed to invoke GPU Headroom API call.https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httml02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE present. CVE ID : CVE-2024-33063https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin. httml02-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33065https:// docs.qua lcomm.c

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
	d9326_firmwa	ire			
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCD9- 241224/2501
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2502
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	0-QUA-WCD9- 241224/2503

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
	d9330_firmwa	ire			
Affected Ver	sion(s): -			1	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2504
Product: wo	d9335_firmwa	ire			
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCD9- 241224/2505
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	0-QUA-WCD9- 241224/2506

4-5

5-6

6-7

7-8

8-9

9-10

3-4

2-3

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2507
02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2508
	ire			
sion(s): -				
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	O-QUA-WCD9- 241224/2509
	02-Dec-2024 02-Dec-2024 02-Dec-2024	02-Dec-2024 7.8 02-Dec-2024 7.5 02-Dec-2024 7.5	O2-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-4305202-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063vd9340_firmwareKemory corruption while Configuring the SMR/S2CR register in Bypass mode.	02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httm02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httml02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE present. CVE ID : CVE-2024-33063https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin. httmldd9340_firmwareMemory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCD9- 241224/2510
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2511
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-WCD9- 241224/2512

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Product: wo	cd9341_firmwa	are			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2513
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCD9- 241224/2514
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-WCD9- 241224/2515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2516
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2517
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2518

0-1

1-2

Page 1071 of 1137

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2519
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2520
Product: wo	d9360_firmwa	are		•	
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2522
	d9370_firmwa	ire			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCD9- 241224/2523
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2524

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCD9- 241224/2525
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2526
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2527
Integer Overflow or CVSSv3 Scoring	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-WCD9- 241224/2528 8-9 9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparoun d			than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2529
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2530
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	O-QUA-WCD9- 241224/2531

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				lletin/de cember- 2024- bulletin. html				
Product: wo	d9371_firmwa	ire						
Affected Ver	sion(s): -			T				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2532			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2533			
Product: wcd9375_firmware								
Affected Version(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso	O-QUA-WCD9- 241224/2534			

 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

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			urces/se curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2535
02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2536
02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-	O-QUA-WCD9- 241224/2537
	02-Dec-2024	02-Dec-2024 7.8 02-Dec-2024 7.8 02-Dec-2024 7.8	O2-Dec-20247.8Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-4304802-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-4305002-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	02-Dec-20247.8Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048urces/se curitybu licerso urces/se curitybu lietin/de cember- 2024. bulletin. httml02-Dec-20247.8Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048https:// docs.qua locers/se curitybu lietin/de cember- 2024. bulletin. httml02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050https:// docs.qua locember- 2024. bulletin. httml02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember-2024-bulletin. httml02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-430522https:// docs.qua lcomm.c om/pro

*stands for all versions

				2024	
				2024- bulletin. html	
Integer Overflow or 0 Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCD9- 241224/2538
Use After Free 0	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCD9- 241224/2539
Product: wcd9	9378_firmwa	re			
Affected Versio	on(s): -				
Stack- based Buffer Overflow)2-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-WCD9- 241224/2540
CVSSv3 Scoring Sca *stands for all vers		1-2 2	- <mark>3</mark> 3-44-55-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Product: wo	cd9380_firmwa	ire			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2541
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2542
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-WCD9- 241224/2543

3-4 4-5

5-6

6-7

7-8

8-9

9-10

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCD9- 241224/2544
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCD9- 241224/2545
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2546

 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
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCD9- 241224/2547
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCD9- 241224/2548
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2549
Use After Free CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-WCD9- 241224/2550 8-9 9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33053	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2551
Product: wo	d9385_firmwa	ire			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCD9- 241224/2552
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call.	https:// docs.qua lcomm.c om/pro duct/pu	0-QUA-WCD9- 241224/2553

3-4

2-3

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-43048	blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCD9- 241224/2554
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCD9- 241224/2555
Improper Input Validation CVSSv3 Scoring	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	0-QUA-WCD9- 241224/2556 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2557
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCD9- 241224/2558
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2559

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
Product: wo	Product: wcd9390_firmware									
Affected Version(s): -										
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2560					
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2561					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2562					

3-4 4-5

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2563
	d9395_firmwa	ire			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2564
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCD9- 241224/2565

0-1

1-2

Page 1086 of 1137

3-4

2-3

4-5

5-6

6-7

7-8

8-9

Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.gua icom.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin html0-QUA-WCD9- 241224/2566Integer Overflow or or Overflow or d02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which htmlhttps:// docs.gua icom.c om/pro duct/pu blicreso curitybu0-QUA-WCD9- 241224/2567Product: wcn3610_firmwareTransient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which html0-QUA-WCD9- 241224/2567Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-430520-QUA-WCN3- 2024- bulletin. https:// docs.gua icomm.c om/pro duct/pu blicreso ucces/se curitybu lletin/de cember- 2024- bulletin. https:// docs.gua icomm.c om/pro duct/pu blicreso ucces/se curitybu lletin/de cember- 2024- bulletin.Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.gua icomm.c om/pro duct/pu blicreso ucces/se curitybu lletin/de cember- 2024- bulletin.Product: wcn3615_firmware91121334455667	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparoun02-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063docs.qua icomm.c om/pro duitive 2024- builetin. html0-QUA-WCD9- 241224/2567Product: wcJ610_firmwcWIUCVE ID : CVE-2024-33063docs.qua icomer- 2024- builetin. html0-QUA-WCD9- 241224/2567Affected VersurewcWIUCVE ID : CVE-2024-33063https:// om/pro duct/pu blicreso urces/se com/pro duct/pu blicreso urces/se trees/se CVE ID : CVE-2024-43052https:// om/pro duct/pu blicreso urces/se<	Input	02-Dec-2024	7.8	processing API calls to NPU with invalid input.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	
Affected Version(s): - Improper Input 02-Dec-2024 7.8 Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052 Validation CVESV3 Scoring Scale 0-1 12 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Overflow or Wraparoun	02-Dec-2024	7.5	parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	=
Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-WCN3- 241224/2568Product: wc3615_firmwareCVSSv3 Scoring Scale0-11-22-33-44-55-66-77-88-99-10	Product: wo	m3610_firmwa	ire		<u> </u>	
Improper Input Validation02-Dec-20247.8Remory corruption while processing API calls to NPU with invali CVE ID : CVE-2024-43052docs.qua lcom.c oduct/pu blicreso ucces/se Curitybu lletin/de cember- 2024- bulletin. html0-QUA-WCN3- 241224/2568Product: www.sets firmwereCVSSv3 Scoring Scale0-11-22-33-44-55-66-77.88-99-10	Affected Ver	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	Input Validation			processing API calls to NPU with invalid input.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•
	Product: wo	m3615_firmwa	ire		•	
			1-2 2	<mark>-3</mark> 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 Version(s): -								
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2569			
	m3620_firmwa	ire						
Affected Ver	sion(s): -							
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2570			
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2571			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2572
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2573
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2574
Improper Restriction of Operations CVSSv3 Scoring	02-Dec-2024 Scale 0-1	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-WCN3- 241224/2575 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			target diagnostic information. CVE ID : CVE-2024-43053	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2576
Product: wo	cn3660b_firmv	vare		1	
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2577
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call.	https:// docs.qua lcomm.c om/pro duct/pu	0-QUA-WCN3- 241224/2578

4-5

5-6

6-7

7-8

8-9

9-10

3-4

2-3

Weakness	Publish Date	CVSSv3	Descrip	tion & C	/E ID	Pa	tch	NCII	PC ID
			CVE ID : CV	Æ-2024	-43048	blicr urce curit lletin cem 2024 bulle htm	s/se tybu n/de ber- 4- etin.		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory co invoking IO user space private con WLAN driv CVE ID : CV	CTL call to set ge nmand in er.	s from neric nside	lcom om/ duct blicr urce curit	a.qua nm.c pro /pu reso s/se tybu n/de ber- 4- etin.	0-QUA- 241224	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory co invoking IO user space test comma driver. CVE ID : CV	CTL call to issue and insid	s from factory le WLAN	lcom om/ duct blicr urce curit	a.qua nm.c pro /pu reso s/se tybu n/de ber- 4- etin.	0-QUA- 241224	
Improper Input Validation CVSSv3 Scoring	02-Dec-2024 Scale 0-1	7.8	Memory co processing with invalio CVE ID : CV	API calls d input.	s to NPU	lcom om/ duct blicr urce curit	s.qua nm.c pro /pu reso es/se	0-QUA- 241224	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember- 2024- bulletin. html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2582
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2583
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2585				
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2586				
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2587				
	Product: wcn3680b_firmware								
Affected Ver	sion(s): -								

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2588
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2589
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2590
Use After Free CVSSv3 Scoring	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as	https:// docs.qua lcomm.c om/pro 6-7 7-8	O-QUA-WCN3- 241224/2591 8-9 9-10

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
		race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html						
02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2592					
02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2593					
Product: wcn3680_firmware Affected Version(s): -									
02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu	O-QUA-WCN3- 241224/2594					
	02-Dec-2024 02-Dec-2024 02-Dec-2024	02-Dec-2024 6.7 02-Dec-2024 6.1 02-Dec-2024 6.1	Image: constraint of the system of the sys	02-Dec-20246.1race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httml02-Dec-20246.7Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-33037https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. httml02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua lcomm.c om/pro					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
	cn3950_firmwa	are			
Affected Ver	sion(s): -			https://	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2595
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2596
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead	https:// docs.qua lcomm.c om/pro duct/pu blicreso	0-QUA-WCN3- 241224/2597

4-5

5-6

6-7

7-8

8-9

9-10

3-4

2-3

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	urces/se curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCN3- 241224/2598
02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2599
	ire			
sion(s): -				
02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	0-QUA-WCN3- 241224/2600
	02-Dec-2024 02-Dec-2024	02-Dec-2024 6.7 02-Dec-2024 6.7 02-Dec-2024 6.1	Image: Constraint of the systemImage: Constraint of the system02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-3305302-Dec-20246.7Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message received from the firmware. CVE ID : CVE-2024-3303702-Dec-20246.1Memory corruption while Configuring the SMR/S2CR register in Bypass mode.	02-Dec-20246.1to huge allocation or invalid memory access. CVE ID : CVE-2024-33036urces/se curitybu lletin/de cember- 2024- bulletin. httm02-Dec-20246.7Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053https:// docs.qua lcomm.c om/pro duct/pu blicreso02-Dec-20246.7Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn't validate the IPC message to NPU driver as the driver doesn't validate the IPC message to NPU driver as the driver doesn't validate the IPC message to NPU driver as the driver doesn't validate the IPC message to NPU driver as the driver doesn't validate the IPC message to NPU dlicreso ures/se curitybu lletin/de cember- 2024- bulletin. httm02-Dec-20248.4Memory corruption while Cofiguring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044https:// docs.qua loom.c om/pro

			curitybu	
			lletin/de cember- 2024- bulletin. html	
02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2601
02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2602
02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-WCN3- 241224/2603
	02-Dec-2024	02-Dec-2024 6.7 02-Dec-2024 6.7	D2-Dec-20247.8processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052D2-Dec-20246.7Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036D2-Dec-20246.7Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	D2-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-430522docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu letin./de cember- 2024- bulletin. httmlD2-Dec-20246.7Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin./de cember- 2024-D2-Dec-20246.7Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocation or invalid memory access. CVE ID : CVE-2024-33036https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin. htmlD2-Dec-20246.7Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin./de cember- 2024-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2604
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2605
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2606
Product: wo	cn3988_firmwa	ire	L	I	l
CVSSv3 Scoring	Scale 0-1	1-2 2	<mark>-3 3-4 4-5 5-6</mark>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Version(s): -								
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2607			
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2608			
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2609			
Use of Out- of-range	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in	https:// docs.qua	0-QUA-WCN3- 241224/2610			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer Offset			camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2611
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2612
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso	0-QUA-WCN3- 241224/2613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/se curitybu lletin/de cember- 2024- bulletin. html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2614
Product: wo	cn3990_firmwa	are			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCN3- 241224/2615
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	0-QUA-WCN3- 241224/2616

0-1

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			curitybu lletin/de cember- 2024- bulletin. html	
02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2617
02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN3- 241224/2618
m3999_firmwa	ire			
sion(s): -				
02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	O-QUA-WCN3- 241224/2619
	02-Dec-2024 02-Dec-2024 02-Dec-2024	02-Dec-2024 7.8 02-Dec-2024 7.5 02-Dec-2024 7.5	O2-Dec-20247.8Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-4304802-Dec-20247.5Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-3306302-Dec-20248.4Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	Image: Constraint of the second sec

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Product: wo	cn6740_firmwa	ire			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN6- 241224/2620
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN6- 241224/2621
Product: wo	cn6755_firmwa	ire			I
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso	0-QUA-WCN6- 241224/2622

urces/se curitybu lletin/de cember- 2024- bulletin. html	
assed to room API blicreso urces/se curitybu 0-QUA-WCN 241224/262	
lls to NPU blicreso 0-QUA-WCN t. curitybu 241224/262	
when a lcomm.c mon info om/pro E greater duct/pu 0-QUA-WCN side which blicreso 241224/262 esent. urces/se	
	on when assed to room API 24-43048 (24-43048) on while lletin/de cember- 2024- bulletin. html https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html https:// https:// https:// adocs.qua letin/de cember- 2024- bulletin. html o-QUA-WCN 241224/262 0-QUA-WCN 241224/262 0-QUA-WCN 241224/262 0-QUA-WCN 241224/262 0-QUA-WCN 241224/262 0-QUA-WCN 241224/262 0-QUA-WCN 241224/262 0-QUA-WCN 241224/262 0-QUA-WCN 241224/262 0-QUA-WCN 241224/262 0-QUA-WCN 241224/262 0-QUA-WCN 241224/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
				2024- bulletin. html					
Product: wo	Product: wcn7860_firmware								
Affected Ver	sion(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN7- 241224/2626				
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN7- 241224/2627				
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-WCN7- 241224/2628				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN7- 241224/2629
	m7861_firmwa	are			
Affected Ver	sion(s): -			1	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN7- 241224/2630
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-WCN7- 241224/2631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN7- 241224/2632
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN7- 241224/2633
	cn7880_firmwa	ire			
Affected Ver	sion(s): -				
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	O-QUA-WCN7- 241224/2634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN7- 241224/2635
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN7- 241224/2636
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCN7- 241224/2637
Product: wc	m7881_firmwa	are			
CVSSv3 Scoring		1-2 2	<mark>-3 3-4 4-5 5-6</mark>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Version(s): -								
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCN7- 241224/2638			
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WCN7- 241224/2639			
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	O-QUA-WCN7- 241224/2640			
Integer Overflow	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a	https:// docs.qua	0-QUA-WCN7- 241224/2641			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparoun d			beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Product: ws	a8810_firmwa	ire			
Affected Vers	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2642
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2643
Stack- based	02-Dec-2024	7.8	Memory corruption when invalid input is passed to	https:// docs.qua lcomm.c	0-QUA-WSA8- 241224/2644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			invoke GPU Headroom API call. CVE ID : CVE-2024-43048	om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2645
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2646
Use of Out- of-range Pointer Offset CVSSv3 Scoring	02-Dec-2024 Scale 0-1	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se	0-QUA-WSA8- 241224/2647 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	curitybu lletin/de cember- 2024- bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2648
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2649
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-WSA8- 241224/2650
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
				bulletin. html	
Product: ws	a8815_firmwa	ire			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2651
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2652
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-WSA8- 241224/2653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2654
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2655
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2656

3-4 4-5

5-6

6-7

7-8

8-9

9-10

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2657
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2658
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2659
	a8830_firmwa	ire			
Affected Ver	sion(s): -				

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2660
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2661
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2662
Improper Restriction of Operations CVSSv3 Scoring	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-WSA8- 241224/2663 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			private command inside WLAN driver. CVE ID : CVE-2024-43049	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2664
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2665
Integer Overflow or Wraparoun d	02-Dec-2024 Scale 0-1	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	0-QUA-WSA8- 241224/2666 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2667
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2668
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-WSA8- 241224/2669

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
				bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2670
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2671
	a8832_firmwa	ire			
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-WSA8- 241224/2672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2673
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2674
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2675

CVSSv3 Scoring Scale0-11-22-33-44-55-6*stands for all versions

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2676
	a8835_firmwa	ire			
Affected Vers	sion(s): -			http://	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2677
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2678

0-1

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

				https://	
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2679
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2680
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2681
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input.	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-WSA8- 241224/2682 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-43052	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2683
Use of Out- of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. CVE ID : CVE-2024-33036	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2684
Untrusted Pointer Dereferenc e	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. CVE ID : CVE-2024-33039	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	O-QUA-WSA8- 241224/2685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. CVE ID : CVE-2024-33040	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2686
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. CVE ID : CVE-2024-33053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2687
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. CVE ID : CVE-2024-33037	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-WSA8- 241224/2688

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
				bulletin. html	
Product: ws	a8840_firmwa	ire			
Affected Ver	sion(s): -				
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2689
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2690
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024-	0-QUA-WSA8- 241224/2691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin. html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2692
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2693
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2694

 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
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2695
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2696
Product: ws	a8845h_firmw	are		•	
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2698
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2699
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2700
Stack- based Buffer Overflow CVSSv3 Scoring	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory	https:// docs.qua lcomm.c om/pro 6-7 7-8	0-QUA-WSA8- 241224/2701 8-9 9-10

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			test command inside WLAN driver. CVE ID : CVE-2024-43050	duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2702
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2703
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu	0-QUA-WSA8- 241224/2704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/de cember- 2024- bulletin. html	
	sa8845_firmwa	ire			
Affected Ver	sion(s): -			1	
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. CVE ID : CVE-2024-33044	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2705
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. CVE ID : CVE-2024-33056	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2706
Stack- based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. CVE ID : CVE-2024-43048	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de	0-QUA-WSA8- 241224/2707

0-1

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

Improper Restriction of Operations within the Bounds of a Memory02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049https:// docs.qua lcomm.c om/pro duct/pu bliereso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-WSA8- 241224/2708Stack- based Buffer02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050https:// docs.qua lcomm.c om/pro duct/pu bliereso urces/se curitybu lletin/de cember- 2024- bulletin. html0-QUA-WSA8- 241224/2708Improper Input Validation0.2-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-430500-QUA-WSA8- 241224/2709Improper Input Validation0.2-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-430520-QUA-WSA8- 2024- bulletin. http:// docs.qua lcomm.c om/pro duct/pu bliereso urces/se curitybu lletin/de cember- 2024- bulletin. http:// docs.qua lcomm.c	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. CVE ID : CVE-2024-43049docs.qua lcompro duct/pu blicreso urces/se curitybu letin/de cember- 2024- bulletin. html0-QUA-WSA8- 241224/2708Stack- based Buffer02-Dec-20247.8Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. CVE ID : CVE-2024-43050https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se0-QUA-WSA8- 241224/2709Improper Improper Imput Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se urces/se					2024- bulletin.	
Stack- based Buffer Overflow02-Dec-20247.8Memory corruption while 	Restriction of Operations within the Bounds of a Memory	02-Dec-2024	7.8	invoking IOCTL calls from user space to set generic private command inside WLAN driver.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•
Improper Input Validation02-Dec-20247.8Memory corruption while processing API calls to NPU with invalid input. CVE ID : CVE-2024-43052docs.qua lcomm.c duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de bulletin.	based Buffer	02-Dec-2024	7.8	invoking IOCTL calls from user space to issue factory test command inside WLAN driver.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•
	Input	02-Dec-2024	7.8	processing API calls to NPU with invalid input.	docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin.	•

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. CVE ID : CVE-2024-43053	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2711
Integer Overflow or Wraparoun d	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. CVE ID : CVE-2024-33063	https:// docs.qua lcomm.c om/pro duct/pu blicreso urces/se curitybu lletin/de cember- 2024- bulletin. html	0-QUA-WSA8- 241224/2712
Vendor: ruij	jienetworks				
Product: rey					
Affected Vers	sion(s): From (i	ncluding)	2.206.0 Up to (excluding) 2.32	20.0	
Server- Side Request Forgery (SSRF)	06-Dec-2024	9.8	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x could give attackers the ability to force Ruijie's proxy servers to perform any request the attackers choose. Using this, attackers could access internal services used by Ruijie and their internal cloud infrastructure via AWS cloud metadata services.	N/A	O-RUI-REYE- 241224/2713

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-48874		
Use of Inherently Dangerous Function	06-Dec-2024	9.8	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x uses an inherently dangerous function which could allow an attacker to send a malicious MQTT message resulting in devices executing arbitrary OS commands. CVE ID : CVE-2024-52324	N/A	O-RUI-REYE- 241224/2714
Weak Password Recovery Mechanism for Forgotten Password	06-Dec-2024	9.4	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x contains a weak mechanism for its users to change their passwords which leaves authentication vulnerable to brute force attacks. CVE ID : CVE-2024-47547	N/A	O-RUI-REYE- 241224/2715
Improper Handling of Insufficient Permission s or Privileges	06-Dec-2024	8.1	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x could allow MQTT clients connecting with device credentials to send messages to some topics. Attackers with device credentials could issue commands to other devices on behalf of Ruijie's cloud. CVE ID : CVE-2024-46874	N/A	O-RUI-REYE- 241224/2716
Insecure Storage of Sensitive Informatio n	06-Dec-2024	7.5	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x could enable an attacker to correlate a device serial number and the user's phone number and part of the email address.	N/A	O-RUI-REYE- 241224/2717

3-4

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-47043		
N/A	06-Dec-2024	7.5	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x uses weak credential mechanism that could allow an attacker to easily calculate MQTT credentials. CVE ID : CVE-2024-45722	N/A	O-RUI-REYE- 241224/2718
Improper Neutralizat ion of Wildcards or Matching Symbols	06-Dec-2024	7.5	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x could allow an attacker to subscribe to partial possible topics in Ruijie MQTT broker, and receive partial messages being sent to and from devices. CVE ID : CVE-2024-47791	N/A	O-RUI-REYE- 241224/2719
Exposure of Private Personal Informatio n to an Unauthoriz ed Actor	06-Dec-2024	6.5	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x contains a a feature that could enable sub accounts or attackers to view and exfiltrate sensitive information from all cloud accounts registered to Ruijie's services CVE ID : CVE-2024-42494	N/A	O-RUI-REYE- 241224/2720
Premature Release of Resource During Expected Lifetime	06-Dec-2024	6.5	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x contains a feature that could enable attackers to invalidate a legitimate user's session and cause a denial-of- service attack on a user's account. CVE ID : CVE-2024-51727	N/A	O-RUI-REYE- 241224/2721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Transmissi on of Private Resources into a New Sphere ('Resource Leak')	06-Dec-2024	6.5	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x could allow an attacker to obtain the devices serial number if physically adjacent and sniffing the RAW WIFI signal. CVE ID : CVE-2024-47146	N/A	O-RUI-REYE- 241224/2722			
Vendor: tot	olink			I	I			
Product: ex1800t_firmware								
Affected Version(s): 9.1.0cu.2112_b20220316								
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Dec-2024	4.3	A vulnerability classified as problematic was found in TOTOLINK EX1800T 9.1.0cu.2112_B20220316. This vulnerability affects the function sub_40662C of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ssid leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12352	N/A	O-TOT-EX18- 241224/2723			
Vendor: Tp-	-link	<u> </u>		I				
Product: vn	020_f3v_firmw	are						
Affected Ver	sion(s): 6.2.102	1						
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Dec-2024	6.5	A vulnerability classified as critical has been found in TP-Link VN020 F3v(T) TT_V6.2.1021. Affected is an unknown function of the file /control/WANIPConnection of the component SOAP Request Handler. The manipulation of the	https:// www.tp- link.com /	O-TPVN02- 241224/2724			

3-4

2-3

4-5

5-6

6-7

7-8

8-9

9-10

CVSSv3 Scoring Scale *stands for all versions

0-1

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument NewConnectionType leads to buffer overflow. The attack needs to be done within the local network. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12343		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Dec-2024	6.3	A vulnerability, which was classified as critical, was found in TP-Link VN020 F3v(T) TT_V6.2.1021. This affects an unknown part of the component FTP USER Command Handler. The manipulation leads to memory corruption. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. CVE ID : CVE-2024-12344	N/A	O-TPVN02- 241224/2725

0-1

1-2

3-4

2-3

4-5

5-6

6-7

7-8

8-9