National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
01 – 15 Sep 2024 Vol. 11 No. 17
https://nciipc.gov.in/

Table of Content

Vendor	Product	Page Number
Qualcomm	immersive_home_214	392
	immersive_home_216	393
	immersive_home_316	393
	immersive_home_318	394
	immersive_home_3210	395
	immersive_home_326	396
	ipq4018	397
	ipq4019	397
	ipq4028	398
	ipq4029	398
	ipq5010	398
	ipq5028	399
	ipq5300	400
	ipq5302	401
	ipq5312	402
	ipq5332	402
	ipq6000	403
	ipq6010	404
	ipq6018	405
	ipq6028	406
	ipq8064	406
	ipq8065	407
	ipq8068	407
	ipq8070a	407
	ipq8071a	408
	ipq8072a	409
	ipq8074a	410
	ipq8076	411
	ipq8076a	412
	ipq8078	413
	ipq8078a	413
	ipq8173	414

Vendor	Product	Page Number
Qualcomm	smart_display_200	643
	snapdragon_1200_wearable	644
	snapdragon_208	644
	snapdragon_210	645
	snapdragon_212	645
	snapdragon_212_mobile	645
	snapdragon_425	646
	snapdragon_425_mobile	646
	snapdragon_429	646
	snapdragon_429_mobile	646
	snapdragon_439	647
	snapdragon_439_mobile	648
	snapdragon_460	648
	snapdragon_460_mobile	649
	snapdragon_480\+_5g	649
	snapdragon_480\+_5g_mobile	650
	snapdragon_480_5g	651
	snapdragon_480_5g_mobile	652
	snapdragon_4_gen_1	652
	snapdragon_4_gen_1_mobile	653
	snapdragon_4_gen_2	654
	snapdragon_4_gen_2_mobile	655
	snapdragon_625	656
	snapdragon_625_mobile	656
	snapdragon_626	656
	snapdragon_626_mobile	656
	snapdragon_630	656
	snapdragon_630_mobile	657
	snapdragon_632	657
	snapdragon_632_mobile	657
	snapdragon_636	658
	snapdragon_636_mobile	658

Vendor	Product	Page Number
Qualcomm	snapdragon_660	658
	snapdragon_660_mobile	659
	snapdragon_662	659
	snapdragon_662_mobile	660
	snapdragon_665	660
	snapdragon_670	661
	snapdragon_670_mobile	661
	snapdragon_675	662
	snapdragon_675_mobile	662
	snapdragon_678	663
	snapdragon_678_mobile	663
	snapdragon_680_4g	663
	snapdragon_680_4g_mobile	664
	snapdragon_685_4g	665
	snapdragon_685_4g_mobile	666
	snapdragon_690_5g	666
	snapdragon_690_5g_mobile	667
	snapdragon_695_5g	667
	snapdragon_695_5g_mobile	668
	snapdragon_6_gen_1	669
	snapdragon_6_gen_1_mobile	669
	snapdragon_710	669
	snapdragon_710_mobile	669
	snapdragon_712	670
	snapdragon_720g	670
	snapdragon_720g_mobile	671
	snapdragon_730	671
	snapdragon_730g	672
	snapdragon_730g_mobile	672
	snapdragon_730_mobile	672
	snapdragon_732g	673
	snapdragon_732g_mobile	673

Vendor	Product	Page Number
Qualcomm	snapdragon_750g_5g	674
	snapdragon_750g_5g_mobile	674
	snapdragon_765g_5g	674
	snapdragon_765g_5g_mobile	675
	snapdragon_765_5g	675
	snapdragon_765_5g_mobile	675
	snapdragon_768g_5g	676
	snapdragon_768g_5g_mobile	676
	snapdragon_778g\+_5g	677
	snapdragon_778g\+_5g_mobile	678
	snapdragon_778g_5g	678
	snapdragon_778g_5g_mobile	679
	snapdragon_780g_5g	680
	snapdragon_780g_5g_mobile	680
	snapdragon_782g	681
	snapdragon_782g_mobile	682
	snapdragon_7c\+_gen_3	683
	snapdragon_7c\+_gen_3_compute	683
	snapdragon_7c_compute	684
	snapdragon_7c_gen_2_compute	684
	snapdragon_7\+_gen_2	685
	snapdragon_7\+_gen_2_mobile	685
	snapdragon_7_gen_1	685
	snapdragon_7_gen_1_mobile	685
	snapdragon_820_automotive	686
	snapdragon_835_mobile_pc	686
	snapdragon_835_pc	687
	snapdragon_845	688
	snapdragon_845_mobile	688
	snapdragon_850_compute	688
	snapdragon_855	689
	snapdragon_855\+	689

Vendor	Product	Page Number
Qualcomm	snapdragon_855\+_mobile	690
	snapdragon_855_mobile	690
	snapdragon_860	690
	snapdragon_860_mobile	691
	snapdragon_865\+_5g	691
	snapdragon_865\+_5g_mobile	692
	snapdragon_865_5g	692
	snapdragon_865_5g_mobile	693
	snapdragon_870_5g	693
	snapdragon_870_5g_mobile	694
	snapdragon_888\+_5g	695
	snapdragon_888\+_5g_mobile	695
	snapdragon_888_5g	696
	snapdragon_888_5g_mobile	697
	snapdragon_8cx_compute	697
	snapdragon_8cx_gen_2_5g_compute	698
	snapdragon_8cx_gen_3	698
	snapdragon_8cx_gen_3_compute	698
	snapdragon_8c_compute	698
	snapdragon_8\+_gen_1	699
	snapdragon_8\+_gen_1_mobile	700
	snapdragon_8\+_gen_2	700
	snapdragon_8\+_gen_2_mobile	701
	snapdragon_8_gen_1	703
	snapdragon_8_gen_1_mobile	704
	snapdragon_8_gen_2	705
	snapdragon_8_gen_2_mobile	705
	snapdragon_8_gen_3	707
	snapdragon_8_gen_3_mobile	708
	snapdragon_ar2_gen_1	709
	snapdragon_auto_4g	711
	snapdragon_auto_5g-rf	712

Vendor	Product	Page Number
Qualcomm	snapdragon_auto_5g-rf_gen_2	712
	snapdragon_auto_5g_modem-rf	712
	snapdragon_auto_5g_modem-rf_gen_2	713
	snapdragon_w5\+_gen_1	715
	snapdragon_w5\+_gen_1_wearable	715
	snapdragon_wear_2100	716
	snapdragon_wear_2500	716
	snapdragon_wear_3100	717
	snapdragon_x12_lte	717
	snapdragon_x20_lte	718
	snapdragon_x35_5g-rf_system	718
	snapdragon_x35_5g_modem-rf	718
	snapdragon_x35_5g_modem-rf_system	719
	snapdragon_x50_5g-rf_system	719
	snapdragon_x50_5g_modem-rf_system	720
	snapdragon_x55_5g-rf_system	720
	snapdragon_x55_5g_modem-rf_system	720
	snapdragon_x5_lte	721
	snapdragon_x62_5g-rf_system	722
	snapdragon_x62_5g_modem-rf	722
	snapdragon_x62_5g_modem-rf_system	722
	snapdragon_x65_5g-rf_system	723
	snapdragon_x65_5g_modem-rf	723
	snapdragon_x65_5g_modem-rf_system	723
	snapdragon_x72_5g-rf_system	724
	snapdragon_x72_5g_modem-rf	725
	snapdragon_x72_5g_modem-rf_system	725
	snapdragon_x75_5g-rf_system	726
	snapdragon_x75_5g_modem-rf	726
	snapdragon_x75_5g_modem-rf_system	727
	snapdragon_xr1	728
	snapdragon_xr2\+_gen_1	728

Vendor	Product	Page Number
Qualcomm	snapdragon_xr2_5g	729
	srv1h	730
	srv1l	732
	srv1m	733
	ssg2115p	735
	ssg2125p	736
	sw5100	738
	sw5100p	740
	sxr1120	741
	sxr1230p	742
	sxr2130	744
	sxr2230p	744
	sxr2250p	746
	talynplus	748
	video_collaboration_vc1	749
	video_collaboration_vc3	751
	video_collaboration_vc5	754
	vision_intelligence_100	756
	vision_intelligence_200	756
	vision_intelligence_300	757
	vision_intelligence_400	757
	wcd9326	759
	wcd9330	759
	wcd9335	760
	wcd9340	762
	wcd9341	764
	wcd9360	766
	wcd9370	766
	wcd9371	769
	wcd9375	769
	wcd9378	772
	wcd9380	772

Vendor	Product	Page Number
Zyxel	nr7303	921
	nr7501	922
	nwa110ax	922
	nwa1123-ac_pro	923
	nwa1123acv3	924
	nwa130be	925
	nwa210ax	926
	nwa220ax-6e	927
	nwa50ax	928
	nwa50ax_pro	928
	nwa55axe	929
	nwa90ax	930
	nwa90ax_pro	931
	pm3100-t0	932
	pm5100-t0	932
	pm7300-t0	933
	px3321-t1	933
	scr50axe	934
	usg_20w-vpn	934
	usg_flex_100	939
	usg_flex_100ax	945
	usg_flex_100w	950
	usg_flex_200	956
	usg_flex_50	961
	usg_flex_500	966
	usg_flex_50w	972
	usg_flex_700	977
	usg_lite_60ax	983
	vmg3625-t50b	984
	vmg3927-t50k	984
	vmg4005-b50a	985
	vmg4005-b60a	985

Vendor	Product	Page Number
Qualcomm	205_mobile_firmware	1904
	215_firmware	1904
	215_mobile_firmware	1904
	315_5g_iot_firmware	1905
	9206_lte_firmware	1905
	apq8017_firmware	1905
	aqt1000_firmware	1906
	ar8031_firmware	1907
	ar8035_firmware	1907
	ar9380_firmware	1909
	c-v2x_9150_firmware	1909
	csr8811_firmware	1910
	csra6620_firmware	1910
	csra6640_firmware	1911
	csrb31024_firmware	1913
	fastconnect_6200_firmware	1913
	fastconnect_6700_firmware	1914
	fastconnect_6800_firmware	1917
	fastconnect_6900_firmware	1918
	fastconnect_7800_firmware	1920
	flight_rb5_5g_firmware	1923
	fsm10055_firmware	1924
	fsm10056_firmware	1925
	fsm20055_firmware	1925
	fsm20056_firmware	1925
	home_hub_100_firmware	1925
	immersive_home_214_firmware	1926
	immersive_home_216_firmware	1927
	immersive_home_316_firmware	1927
	immersive_home_318_firmware	1928
	immersive_home_3210_firmware	1929
	immersive_home_326_firmware	1930

Vendor	Product	Page Number
Qualcomm	ipq4018_firmware	1931
	ipq4019_firmware	1931
	ipq4028_firmware	1932
	ipq4029_firmware	1932
	ipq5010_firmware	1932
	ipq5028_firmware	1933
	ipq5300_firmware	1934
	ipq5302_firmware	1935
	ipq5312_firmware	1936
	ipq5332_firmware	1936
	ipq6000_firmware	1937
	ipq6010_firmware	1938
	ipq6018_firmware	1939
	ipq6028_firmware	1940
	ipq8064_firmware	1940
	ipq8065_firmware	1941
	ipq8068_firmware	1941
	ipq8070a_firmware	1941
	ipq8071a_firmware	1942
	ipq8072a_firmware	1943
	ipq8074a_firmware	1944
	ipq8076a_firmware	1945
	ipq8076_firmware	1946
	ipq8078a_firmware	1946
	ipq8078_firmware	1947
	ipq8173_firmware	1948
	ipq8174_firmware	1949
	ipq9008_firmware	1950
	ipq9554_firmware	1951
	ipq9570_firmware	1951
	ipq9574_firmware	1952
	mdm8215_firmware	1953

Vendor	Product	Page Number
Qualcomm	mdm9215_firmware	1954
	mdm9250_firmware	1954
	mdm9310_firmware	1954
	mdm9615_firmware	1954
	mdm9628_firmware	1955
	mdm9640_firmware	1956
	mdm9645_firmware	1956
	mdm9650_firmware	1956
	msm8108_firmware	1957
	msm8209_firmware	1957
	msm8608_firmware	1958
	msm8909w_firmware	1958
	msm8996au_firmware	1958
	qam8255p_firmware	1959
	qam8295p_firmware	1961
	qam8620p_firmware	1963
	qam8650p_firmware	1964
	qam8775p_firmware	1966
	qamsrv1h_firmware	1968
	qamsrv1m_firmware	1969
	qca0000_firmware	1971
	qca1062_firmware	1972
	qca1064_firmware	1972
	qca2062_firmware	1972
	qca2064_firmware	1972
	qca2065_firmware	1973
	qca2066_firmware	1973
	qca4024_firmware	1973
	qca6174a_firmware	1974
	qca6174_firmware	1975
	qca6175a_firmware	1975
	qca6310_firmware	1976

Vendor	Product	Page Number
Qualcomm	qca6320_firmware	1977
	qca6335_firmware	1978
	qca6391_firmware	1979
	qca6420_firmware	1981
	qca6421_firmware	1981
	qca6426_firmware	1982
	qca6430_firmware	1983
	qca6431_firmware	1984
	qca6436_firmware	1985
	qca6554a_firmware	1986
	qca6564au_firmware	1987
	qca6564a_firmware	1989
	qca6564_firmware	1990
	qca6574au_firmware	1991
	qca6574a_firmware	1993
	qca6574_firmware	1995
	qca6584au_firmware	1997
	qca6584_firmware	1998
	qca6595au_firmware	1999
	qca6595_firmware	2001
	qca6678aq_firmware	2003
	qca6688aq_firmware	2004
	qca6696_firmware	2006
	qca6698aq_firmware	2008
	qca6777aq_firmware	2010
	qca6787aq_firmware	2011
	qca6797aq_firmware	2011
	qca7500_firmware	2013
	qca8075_firmware	2013
	qca8081_firmware	2014
	qca8082_firmware	2016
	qca8084_firmware	2017

Vendor	Product	Page Number
Qualcomm	qca8085_firmware	2018
	qca8337_firmware	2018
	qca8386_firmware	2020
	qca9367_firmware	2021
	qca9377_firmware	2022
	qca9378_firmware	2023
	qca9379_firmware	2023
	qca9880_firmware	2023
	qca9886_firmware	2023
	qca9888_firmware	2024
	qca9889_firmware	2025
	qca9898_firmware	2025
	qca9980_firmware	2026
	qca9984_firmware	2026
	qca9985_firmware	2027
	qca9990_firmware	2027
	qca9992_firmware	2027
	qca9994_firmware	2028
	qcc2073_firmware	2028
	qcc2076_firmware	2029
	qcc710_firmware	2030
	qcf8000_firmware	2031
	qcf8001_firmware	2032
	qcm2150_firmware	2033
	qcm2290_firmware	2034
	qcm4290_firmware	2034
	qcm4325_firmware	2035
	qcm4490_firmware	2037
	qcm5430_firmware	2038
	qcm6125_firmware	2041
	qcm6490_firmware	2042
	qcm8550_firmware	2045

Vendor	Product	Page Number
Qualcomm	qcs2290_firmware	2076
	qcs410_firmware	2077
	qcs4290_firmware	2078
	qcs4490_firmware	2079
	qcs5430_firmware	2081
	qcs610_firmware	2083
	qcs6125_firmware	2085
	qcs6490_firmware	2086
	qcs7230_firmware	2089
	qcs8250_firmware	2091
	qcs8550_firmware	2093
	qdu1000_firmware	2095
	qdu1010_firmware	2095
	qdu1110_firmware	2096
	qdu1210_firmware	2097
	qdx1010_firmware	2097
	qdx1011_firmware	2098
	qep8111_firmware	2098
	qfw7114_firmware	2100
	qfw7124_firmware	2101
	qrb5165m_firmware	2103
	qrb5165n_firmware	2104
	qru1032_firmware	2105
	qru1052_firmware	2106
	qru1062_firmware	2106
	qsm8250_firmware	2107
	qsm8350_firmware	2107
	qxm8083_firmware	2108
	robotics_rb3_firmware	2109
	robotics_rb5_firmware	2110
	sa4150p_firmware	2111
	sa4155p_firmware	2112

Vendor	Product	Page Number
Qualcomm	sd888_firmware	2151
	sdm429w_firmware	2152
	sdx20m_firmware	2154
	sdx55_firmware	2154
	sdx61_firmware	2156
	sdx65m_firmware	2157
	sd_455_firmware	2158
	sd_675_firmware	2158
	sd_8cx_firmware	2158
	sd_8_gen1_5g_firmware	2158
	sg4150p_firmware	2160
	sg8275p_firmware	2161
	sm4125_firmware	2163
	sm4635_firmware	2163
	sm6250p_firmware	2164
	sm6250_firmware	2164
	sm6370_firmware	2165
	sm7250p_firmware	2166
	sm7315_firmware	2167
	sm7325p_firmware	2168
	sm7435_firmware	2170
	sm8550p_firmware	2170
	sm8635_firmware	2172
	sm8750_firmware	2175
	smart_audio_200_firmware	2175
	smart_audio_400_firmware	2176
	smart_display_200_firmware	2177
	snapdragon_1200_wearable_firmware	2177
	snapdragon_208_firmware	2178
	snapdragon_210_firmware	2178
	snapdragon_212_firmware	2179
	snapdragon_212_mobile_firmware	2179

Vendor	Product	Page Number
Qualcomm	snapdragon_425_firmware	2179
	snapdragon_425_mobile_firmware	2179
	snapdragon_429_firmware	2179
	snapdragon_429_mobile_firmware	2180
	snapdragon_439_firmware	2181
	snapdragon_439_mobile_firmware	2181
	snapdragon_460_firmware	2181
	snapdragon_460_mobile_firmware	2182
	snapdragon_480\+_5g_firmware	2183
	snapdragon_480\+_5g_mobile_firmware	2184
	snapdragon_480_5g_firmware	2184
	snapdragon_480_5g_mobile_firmware	2185
	snapdragon_4_gen_1_firmware	2186
	snapdragon_4_gen_1_mobile_firmware	2187
	snapdragon_4_gen_2_firmware	2187
	snapdragon_4_gen_2_mobile_firmware	2188
	snapdragon_625_firmware	2189
	snapdragon_625_mobile_firmware	2189
	snapdragon_626_firmware	2189
	snapdragon_626_mobile_firmware	2190
	snapdragon_630_firmware	2190
	snapdragon_630_mobile_firmware	2190
	snapdragon_632_firmware	2191
	snapdragon_632_mobile_firmware	2191
	snapdragon_636_firmware	2191
	snapdragon_636_mobile_firmware	2191
	snapdragon_660_firmware	2192
	snapdragon_660_mobile_firmware	2192
	snapdragon_662_firmware	2193
	snapdragon_662_mobile_firmware	2193
	snapdragon_665_firmware	2194
	snapdragon_670_firmware	2194

Vendor	Product	Page Number
Qualcomm	snapdragon_670_mobile_firmware	2195
	snapdragon_675_firmware	2195
	snapdragon_675_mobile_firmware	2196
	snapdragon_678_firmware	2196
	snapdragon_678_mobile_firmware	2196
	snapdragon_680_4g_firmware	2197
	snapdragon_680_4g_mobile_firmware	2198
	snapdragon_685_4g_firmware	2198
	snapdragon_685_4g_mobile_firmware	2199
	snapdragon_690_5g_firmware	2200
	snapdragon_690_5g_mobile_firmware	2200
	snapdragon_695_5g_firmware	2201
	snapdragon_695_5g_mobile_firmware	2201
	snapdragon_6_gen_1_firmware	2202
	snapdragon_6_gen_1_mobile_firmware	2202
	snapdragon_710_firmware	2203
	snapdragon_710_mobile_firmware	2203
	snapdragon_712_firmware	2203
	snapdragon_720g_firmware	2204
	snapdragon_720g_mobile_firmware	2204
	snapdragon_730g_firmware	2205
	snapdragon_730g_mobile_firmware	2205
	snapdragon_730_firmware	2205
	snapdragon_730_mobile_firmware	2206
	snapdragon_732g_firmware	2206
	snapdragon_732g_mobile_firmware	2207
	snapdragon_750g_5g_firmware	2207
	snapdragon_750g_5g_mobile_firmware	2207
	snapdragon_765g_5g_firmware	2208
	snapdragon_765g_5g_mobile_firmware	2208
	snapdragon_765_5g_firmware	2208
	snapdragon_765_5g_mobile_firmware	2209

Vendor	Product	Page Number
Qualcomm	snapdragon_768g_5g_firmware	2209
	snapdragon_768g_5g_mobile_firmware	2210
	snapdragon_778g\+_5g_firmware	2210
	snapdragon_778g\+_5g_mobile_firmware	2211
	snapdragon_778g_5g_firmware	2212
	snapdragon_778g_5g_mobile_firmware	2212
	snapdragon_780g_5g_firmware	2213
	snapdragon_780g_5g_mobile_firmware	2214
	snapdragon_782g_firmware	2215
	snapdragon_782g_mobile_firmware	2215
	snapdragon_7c\+_gen_3_compute_firmware	2216
	snapdragon_7c\+_gen_3_firmware	2217
	snapdragon_7c_compute_firmware	2218
	snapdragon_7c_gen_2_compute_firmware	2218
	snapdragon_7\+_gen_2_firmware	2218
	snapdragon_7\+_gen_2_mobile_firmware	2218
	snapdragon_7_gen_1_firmware	2219
	snapdragon_7_gen_1_mobile_firmware	2219
	snapdragon_820_automotive_firmware	2219
	snapdragon_835_mobile_pc_firmware	2220
	snapdragon_835_pc_firmware	2221
	snapdragon_845_firmware	2221
	snapdragon_845_mobile_firmware	2222
	snapdragon_850_compute_firmware	2222
	snapdragon_855\+_firmware	2222
	snapdragon_855\+_mobile_firmware	2223
	snapdragon_855_firmware	2223
	snapdragon_855_mobile_firmware	2223
	snapdragon_860_firmware	2224
	snapdragon_860_mobile_firmware	2224
	snapdragon_865\+_5g_firmware	2225
	snapdragon_865\+_5g_mobile_firmware	2225

Vendor	Product	Page Number
Qualcomm	snapdragon_865_5g_firmware	2226
	snapdragon_865_5g_mobile_firmware	2226
	snapdragon_870_5g_firmware	2227
	snapdragon_870_5g_mobile_firmware	2227
	snapdragon_888\+_5g_firmware	2228
	snapdragon_888\+_5g_mobile_firmware	2229
	snapdragon_888_5g_firmware	2229
	snapdragon_888_5g_mobile_firmware	2230
	snapdragon_8cx_compute_firmware	2231
	snapdragon_8cx_gen_2_5g_compute_firmware	2231
	snapdragon_8cx_gen_3_compute_firmware	2231
	snapdragon_8cx_gen_3_firmware	2231
	snapdragon_8c_compute_firmware	2232
	snapdragon_8\+_gen_1_firmware	2232
	snapdragon_8\+_gen_1_mobile_firmware	2233
	snapdragon_8\+_gen_2_firmware	2234
	snapdragon_8\+_gen_2_mobile_firmware	2235
	snapdragon_8_gen_1_firmware	2236
	snapdragon_8_gen_1_mobile_firmware	2237
	snapdragon_8_gen_2_firmware	2238
	snapdragon_8_gen_2_mobile_firmware	2239
	snapdragon_8_gen_3_firmware	2240
	snapdragon_8_gen_3_mobile_firmware	2241
	snapdragon_ar2_gen_1_firmware	2242
	snapdragon_auto_4g_firmware	2244
	snapdragon_auto_5g-rf_firmware	2245
	snapdragon_auto_5g-rf_gen_2_firmware	2245
	snapdragon_auto_5g_modem-rf_firmware	2245
	snapdragon_auto_5g_modem-rf_gen_2_firmware	2246
	snapdragon_w5\+_gen_1_firmware	2248
	snapdragon_w5\+_gen_1_wearable_firmware	2248
	snapdragon_wear_2100_firmware	2249

Vendor	Product	Page Number
Qualcomm	snapdragon_wear_2500_firmware	2249
	snapdragon_wear_3100_firmware	2250
	snapdragon_x12_lte_firmware	2250
	snapdragon_x20_lte_firmware	2251
	snapdragon_x35_5g-rf_system_firmware	2251
	snapdragon_x35_5g_modem-rf_firmware	2252
	snapdragon_x35_5g_modem-rf_system_firmware	2252
	snapdragon_x50_5g-rf_system_firmware	2253
	snapdragon_x50_5g_modem-rf_system_firmware	2253
	snapdragon_x55_5g-rf_system_firmware	2253
	snapdragon_x55_5g_modem-rf_system_firmware	2254
	snapdragon_x5_lte_firmware	2255
	snapdragon_x62_5g-rf_system_firmware	2255
	snapdragon_x62_5g_modem-rf_firmware	2255
	snapdragon_x62_5g_modem-rf_system_firmware	2255
	snapdragon_x65_5g-rf_system_firmware	2256
	snapdragon_x65_5g_modem-rf_firmware	2256
	snapdragon_x65_5g_modem-rf_system_firmware	2256
	snapdragon_x72_5g-rf_system_firmware	2258
	snapdragon_x72_5g_modem-rf_firmware	2258
	snapdragon_x72_5g_modem-rf_system_firmware	2258
	snapdragon_x75_5g-rf_system_firmware	2259
	snapdragon_x75_5g_modem-rf_firmware	2260
	snapdragon_x75_5g_modem-rf_system_firmware	2260
	snapdragon_xr1_firmware	2261
	snapdragon_xr2\+_gen_1_firmware	2262
	snapdragon_xr2_5g_firmware	2263

Vendor	Product	Page Number
Qualcomm	srv1h_firmware	2263
	srv1l_firmware	2265
	srv1m_firmware	2266
	ssg2115p_firmware	2268
	ssg2125p_firmware	2270
	sw5100p_firmware	2271
	sw5100_firmware	2273
	sxr1120_firmware	2274
	sxr1230p_firmware	2275
	sxr2130_firmware	2277
	sxr2230p_firmware	2278
	sxr2250p_firmware	2279
	talynplus_firmware	2281
	video_collaboration_vc1_firmware	2283
	video_collaboration_vc3_firmware	2284
	video_collaboration_vc5_firmware	2287
	vision_intelligence_100_firmware	2289
	vision_intelligence_200_firmware	2290
	vision_intelligence_300_firmware	2290
	vision_intelligence_400_firmware	2290
	wcd9326_firmware	2292
	wcd9330_firmware	2293
	wcd9335_firmware	2293
	wcd9340_firmware	2295
	wcd9341_firmware	2297
	wcd9360_firmware	2299
	wcd9370_firmware	2300
	wcd9371_firmware	2302
	wcd9375_firmware	2303
	wcd9378_firmware	2305
	wcd9380_firmware	2306
	wcd9385_firmware	2308

Vendor	Product	Page Number
Zyxel	dx5401-b1_firmware	2434
	emg3525-t50b_firmware	2435
	emg5523-t50b_firmware	2435
	emg5723-t50k_firmware	2435
	ex3300-t0_firmware	2436
	ex3300-t1_firmware	2436
	ex3301-t0_firmware	2437
	ex3500-t0_firmware	2437
	ex3501-t0_firmware	2438
	ex3510-b0_firmware	2438
	ex5401-b0_firmware	2439
	ex5401-b1_firmware	2439
	ex5510-b0_firmware	2440
	ex5512-t0_firmware	2440
	ex5601-t0_firmware	2441
	ex5601-t1_firmware	2441
	ex7501-b0_firmware	2442
	ex7710-b0_firmware	2442
	nebula_fwa505_firmware	2443
	nebula_fwa510_firmware	2443
	nebula_fwa710_firmware	2444
	nebula_lte3301-plus_firmware	2444
	nr5103ev2_firmware	2445
	nr5103_firmware	2445
	nr5307_firmware	2446
	nr7103_firmware	2446
	nr7302_firmware	2446
	nr7303_firmware	2447
	nr7501_firmware	2447
	nwa110ax_firmware	2448
	nwa1123-ac_pro_firmware	2449
	nwa1123acv3_firmware	2450

Vendor	Product	Page Number
Zyxel	nwa130be_firmware	2451
	nwa210ax_firmware	2452
	nwa220ax-6e_firmware	2452
	nwa50ax_firmware	2453
	nwa50ax_pro_firmware	2454
	nwa55axe_firmware	2455
	nwa90ax_firmware	2456
	nwa90ax_pro_firmware	2457
	pm3100-t0_firmware	2458
	pm5100-t0_firmware	2458
	pm7300-t0_firmware	2459
	px3321-t1_firmware	2459
	scr50axe_firmware	2460
	usg_lite_60ax_firmware	2460
	vmg3625-t50b_firmware	2461
	vmg3927-t50k_firmware	2461
	vmg4005-b50a_firmware	2462
	vmg4005-b60a_firmware	2462
	vmg8623-t50b_firmware	2463
	vmg8825-t50k_firmware	2463
	wac500h_firmware	2464
	wac500_firmware	2465
	wac6103d-i_firmware	2466
	wac6502d-s_firmware	2466
	wac6503d-s_firmware	2467
	wac6552d-s_firmware	2468
	wac6553d-e_firmware	2469
	wax300h_firmware	2470
	wax510d_firmware	2471
	wax610d_firmware	2472
	wax620d-6e_firmware	2473
	wax630s_firmware	2474

Vendor	Product	Page Number
Zyxel	wax640s-6e_firmware	2474
	wax650s_firmware	2475
	wax655e_firmware	2476
	wbe530_firmware	2477
	wbe660s_firmware	2478
	wx3100-t0_firmware	2479
	wx3401-b0_firmware	2479
	wx5600-t0_firmware	2480
	zld_firmware	2480

Common Vulnerabilities and Exposures(CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 3DS					
Product: 3dexperience					
Affected Version(s): r2023x					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-2024	5.4	A stored Cross-site Scripting (XSS) vulnerability affecting 3DDashboard in 3DSwymer from Release 3DEXPERIENCE R2023x through Release 3DEXPERIENCE R2024x allows an attacker to execute arbitrary script code in user's browser session. **CVE ID: CVE-2024-7938**	https://www.3ds.com/vulnerability/advisories	A-3DS-3DEX-180924/1
Affected Version(s): r2024x					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-2024	5.4	A stored Cross-site Scripting (XSS) vulnerability affecting 3DDashboard in 3DSwymer on Release 3DEXPERIENCE R2024x allows an attacker to execute arbitrary script code in user's browser session. **CVE ID: CVE-2024-7932**	https://www.3ds.com/vulnerability/advisories	A-3DS-3DEX-180924/2

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 Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-2024	5.4	A stored Cross-site Scripting (XSS) vulnerability affecting 3DDashboard in 3DSwymer from Release 3DEXPERIENCE R2023x through Release 3DEXPERIENCE R2024x allows an attacker to execute arbitrary script code in user's browser session. **CVE ID: CVE-2024-7938**	https://www.3ds.com/vulnerability/advisories	A-3DS-3DEX-180924/3
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-2024	5.4	A stored Cross-site Scripting (XSS) vulnerability affecting 3DSwym in 3DSwymer on Release 3DEXPERIENCE R2024x allows an attacker to execute arbitrary script code in user's browser session. **CVE ID: CVE-2024-7939**	https://www.3ds.com/vulnerability/advisories	A-3DS-3DEX-180924/4
Product: 3dexperience_enovia					
Affected Version(s): r2023x					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-2024	5.4	A stored Cross-site Scripting (XSS) vulnerability affecting ENOVIA Collaborative Industry Innovator from Release 3DEXPERIENCE	https://www.3ds.com/vulnerability/advisories	A-3DS-3DEX-180924/5

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R2022x through Release 3DEXPERIENCE R2024x allows an attacker to execute arbitrary script code in user's browser session. **CVE ID: CVE-2024-8004**		
Affected Version(s): r2024x					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-2024	5.4	A stored Cross-site Scripting (XSS) vulnerability affecting ENOVIA Collaborative Industry Innovator from Release 3DEXPERIENCE R2022x through Release 3DEXPERIENCE R2024x allows an attacker to execute arbitrary script code in user's browser session. **CVE ID: CVE-2024-8004**	https://www.3ds.com/vulnerability/advisories	A-3DS-3DEX-180924/6
Affected Version(s): r2022x					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-2024	5.4	A stored Cross-site Scripting (XSS) vulnerability affecting ENOVIA Collaborative Industry Innovator from Release 3DEXPERIENCE R2022x through Release 3DEXPERIENCE R2024x allows an	https://www.3ds.com/vulnerability/advisories	A-3DS-3DEX-180924/7

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
			attacker to execute arbitrary script code in user's browser session. **CVE ID: CVE-2024-8004**		
Vendor: abcd-community					
Product: abcd					
Affected Version(s): 2.2.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Sep-2024	7.5	A vulnerability classified as problematic has been found in ABCD ABCD2 up to 2.2.0-beta-1. This affects an unknown part of the file /common/show_image.php. The manipulation of the argument image leads to path traversal: '../filedir'. It is possible to initiate 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-2024-8409**	N/A	A-ABC-ABCD-180924/8
Improper Limitation of a Pathname	04-Sep-2024	7.5	A vulnerability classified as problematic was found in ABCD	N/A	A-ABC-ABCD-180924/9

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
to a Restricted Directory ('Path Traversal')			ABCD2 up to 2.2.0-beta-1. This vulnerability affects unknown code of the file /abcd/opac/php/otros_sitios.php. The manipulation of the argument sitio leads to path traversal. The attack can 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-2024-8410**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Sep-2024	4.3	A vulnerability, which was classified as problematic, has been found in ABCD ABCD2 up to 2.2.0-beta-1. This issue affects some unknown processing of the file /buscar_integrada.php. The manipulation of the argument Sub_Expresion leads to cross site scripting. The	N/A	A-ABC-ABCD-180924/10

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
			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-2024-8411**		
Vendor: accordors					
Product: accord_ors					
Affected Version(s): * Up to (excluding) 7.3.2.1					
N/A	06-Sep-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Ariva Computer Accord ORS allows Retrieve Embedded Sensitive Data.This issue affects Accord ORS: before 7.3.2.1. **CVE ID: CVE-2024-1744**	N/A	A-ACC-ACCO-180924/11
Vendor: Adobe					
Product: acrobat					
Affected Version(s): From (including) 20.001.30005 Up to (excluding) 20.005.30655					
Use After Free	05-Sep-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20964, 24.001.30123, 24.002.20991 and earlier are affected	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-180924/12

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
			by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-45107**		
Affected Version(s): From (including) 24.001.20604 Up to (excluding) 24.001.30159					
Use After Free	05-Sep-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20964, 24.001.30123, 24.002.20991 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-45107**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-180924/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: acrobat_dc					
Affected Version(s): From (including) 15.007.20033 Up to (excluding) 24.002.21005					
Use After Free	05-Sep-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20964, 24.001.30123, 24.002.20991 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-45107**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-180924/14
Product: acrobat_reader					
Affected Version(s): From (including) 20.001.30005 Up to (excluding) 20.005.30655					
Use After Free	05-Sep-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20964, 24.001.30123, 24.002.20991 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-180924/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-45107**		
Product: acrobat_reader_dc					
Affected Version(s): From (including) 15.007.20033 Up to (excluding) 24.002.21005					
Use After Free	05-Sep-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20964, 24.001.30123, 24.002.20991 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-45107**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	A-ADO-ACRO-180924/16
Product: after_effects					
Affected Version(s): * Up to (excluding) 23.6.9					
Improper Restriction of	13-Sep-2024	7.8	After Effects versions 23.6.6, 24.5 and earlier are	https://helpx.adobe.com/security/products/af	A-ADO-AFTE-180924/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			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-2024-39380**	ter_effects/apsb24-55.html	
Out-of-bounds Write	13-Sep-2024	7.8	After Effects versions 23.6.6, 24.5 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-2024-39381**	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	A-ADO-AFTE-180924/18
Out-of-bounds Write	13-Sep-2024	7.8	After Effects versions 23.6.6, 24.5 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	A-ADO-AFTE-180924/19

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
			context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41859**		
Out-of-bounds Read	13-Sep-2024	5.5	After Effects versions 23.6.6, 24.5 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-2024-39382**	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	A-ADO-AFTE-180924/20
Out-of-bounds Read	13-Sep-2024	5.5	After Effects versions 23.6.6, 24.5 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	A-ADO-AFTE-180924/21

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
			such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41867**		
Affected Version(s): From (including) 24.0 Up to (excluding) 24.6					
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Sep-2024	7.8	After Effects versions 23.6.6, 24.5 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-2024-39380**	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	A-ADO-AFTE-180924/22
Out-of-bounds Write	13-Sep-2024	7.8	After Effects versions 23.6.6, 24.5 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	A-ADO-AFTE-180924/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID: CVE-2024-39381**		
Out-of-bounds Write	13-Sep-2024	7.8	After Effects versions 23.6.6, 24.5 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-2024-41859**	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	A-ADO-AFTE-180924/24
Out-of-bounds Read	13-Sep-2024	5.5	After Effects versions 23.6.6, 24.5 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	A-ADO-AFTE-180924/25

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
			CVE ID: CVE-2024-39382		
Out-of-bounds Read	13-Sep-2024	5.5	After Effects versions 23.6.6, 24.5 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-2024-41867**	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	A-ADO-AFTE-180924/26
Product: coldfusion					
Affected Version(s): 2021					
Deserialization of Untrusted Data	13-Sep-2024	9.8	ColdFusion versions 2023.9, 2021.15 and earlier are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability by providing crafted input to the	https://helpx.adobe.com/security/products/coldfusion/apsb24-71.html	A-ADO-COLD-180924/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application, which when deserialized, leads to execution of malicious code. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-41874**		
Improper Authentication	13-Sep-2024	7.5	ColdFusion versions 2023.6, 2021.12 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access and affect the integrity of the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45113**	https://helpx.adobe.com/security/products/coldfusion/apsb24-14.html	A-ADO-COLD-180924/28
Affected Version(s): 2023					
Deserialization of Untrusted Data	13-Sep-2024	9.8	ColdFusion versions 2023.9, 2021.15 and earlier are affected by a Deserialization of Untrusted Data vulnerability that could result in	https://helpx.adobe.com/security/products/coldfusion/apsb24-71.html	A-ADO-COLD-180924/29

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability by providing crafted input to the application, which when deserialized, leads to execution of malicious code. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-41874**		
Improper Authentication	13-Sep-2024	7.5	ColdFusion versions 2023.6, 2021.12 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access and affect the integrity of the application. Exploitation of this issue does not require user interaction. **CVE ID: CVE-2024-45113**	https://helpx.adobe.com/security/products/coldfusion/apsb24-14.html	A-ADO-COLD-180924/30

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
Product: illustrator					
Affected Version(s): * Up to (excluding) 27.9.6					
Integer Underflow (Wrap or Wraparound)	13-Sep-2024	7.8	Illustrator versions 28.6, 27.9.5 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-2024-41857**	https://helpx.adobe.com/security/products/illustrator/apsb24-66.html	A-ADO-ILLU-180924/31
Affected Version(s): From (including) 27.0.0 Up to (excluding) 27.9.6					
Use After Free	13-Sep-2024	7.8	Illustrator versions 28.6, 27.9.5 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-43758**	https://helpx.adobe.com/security/products/illustrator/apsb24-66.html	A-ADO-ILLU-180924/32
NULL Pointer	13-Sep-2024	5.5	Illustrator versions 28.6, 27.9.5 and earlier are affected	https://helpx.adobe.com/security/products/ill	A-ADO-ILLU-180924/33

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			by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a DoS condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-43759**	ustrator/apsb24-66.html	
Out-of-bounds Read	13-Sep-2024	5.5	Illustrator versions 28.6, 27.9.5 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-2024-45111**	https://helpx.adobe.com/security/products/illustrator/apsb24-66.html	A-ADO-ILLU-180924/34
Affected Version(s): From (including) 28.0 Up to (excluding) 28.7.1					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	13-Sep-2024	7.8	Illustrator versions 28.6, 27.9.5 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-2024-41857**	https://helpx.adobe.com/security/products/illustrator/apsb24-66.html	A-ADO-ILLU-180924/35
Use After Free	13-Sep-2024	7.8	Illustrator versions 28.6, 27.9.5 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-43758**	https://helpx.adobe.com/security/products/illustrator/apsb24-66.html	A-ADO-ILLU-180924/36
NULL Pointer Dereference	13-Sep-2024	5.5	Illustrator versions 28.6, 27.9.5 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an	https://helpx.adobe.com/security/products/illustrator/apsb24-66.html	A-ADO-ILLU-180924/37

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
			application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a DoS condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-43759**		
Out-of-bounds Read	13-Sep-2024	5.5	Illustrator versions 28.6, 27.9.5 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-2024-45111**	https://helpx.adobe.com/security/products/illustrator/apsb24-66.html	A-ADO-ILLU-180924/38
Product: media_encoder					
Affected Version(s): * Up to (excluding) 23.6.9					
Out-of-bounds Write	13-Sep-2024	7.8	Media Encoder versions 24.5, 23.6.8 and earlier	https://helpx.adobe.com/security/products/m	A-ADO-MEDI-180924/39

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
			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-2024-39377**	edia-encoder/apsb24-53.html	
Out-of-bounds Read	13-Sep-2024	7.8	Media Encoder versions 24.5, 23.6.8 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2024-41871**	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	A-ADO-MEDI-180924/40

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
Out-of-bounds Read	13-Sep-2024	5.5	Media Encoder versions 24.5, 23.6.8 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-2024-41870**	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	A-ADO-MEDI-180924/41
Out-of-bounds Read	13-Sep-2024	5.5	Media Encoder versions 24.5, 23.6.8 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-2024-41872**	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	A-ADO-MEDI-180924/42

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
Out-of-bounds Read	13-Sep-2024	5.5	Media Encoder versions 24.5, 23.6.8 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-2024-41873**	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	A-ADO-MEDI-180924/43
Affected Version(s): From (including) 24.0 Up to (excluding) 24.6					
Out-of-bounds Write	13-Sep-2024	7.8	Media Encoder versions 24.5, 23.6.8 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-2024-39377**	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	A-ADO-MEDI-180924/44

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
Out-of-bounds Read	13-Sep-2024	7.8	Media Encoder versions 24.5, 23.6.8 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2024-41871**	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	A-ADO-MEDI-180924/45
Out-of-bounds Read	13-Sep-2024	5.5	Media Encoder versions 24.5, 23.6.8 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	A-ADO-MEDI-180924/46

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
			victim must open a malicious file. **CVE ID: CVE-2024-41870**		
Out-of-bounds Read	13-Sep-2024	5.5	Media Encoder versions 24.5, 23.6.8 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-2024-41872**	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	A-ADO-MEDI-180924/47
Affected Version(s): From (including) 24.0 Up to (including) 24.6					
Out-of-bounds Read	13-Sep-2024	5.5	Media Encoder versions 24.5, 23.6.8 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	A-ADO-MEDI-180924/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-41873**		
Product: photoshop					
Affected Version(s): * Up to (excluding) 24.7.5					
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Sep-2024	7.8	Photoshop Desktop versions 24.7.4, 25.11 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-2024-43756**	https://helpx.adobe.com/security/products/photoshop/apsb24-72.html	A-ADO-PHOT-180924/49
Out-of-bounds Write	13-Sep-2024	7.8	Photoshop Desktop versions 24.7.4, 25.11 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.adobe.com/security/products/photoshop/apsb24-72.html	A-ADO-PHOT-180924/50

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
			CVE ID: CVE-2024-43760		
Out-of-bounds Write	13-Sep-2024	7.8	Photoshop Desktop versions 24.7.4, 25.11 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-2024-45108**	https://helpx.adobe.com/security/products/photoshop/apsb24-72.html	A-ADO-PHOT-180924/51
Out-of-bounds Write	13-Sep-2024	7.8	Photoshop Desktop versions 24.7.4, 25.11 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-2024-45109**	https://helpx.adobe.com/security/products/photoshop/apsb24-72.html	A-ADO-PHOT-180924/52
Affected Version(s): From (including) 25.0 Up to (excluding) 25.12					
Improper Restriction of	13-Sep-2024	7.8	Photoshop Desktop versions 24.7.4, 25.11 and earlier	https://helpx.adobe.com/security/products/p	A-ADO-PHOT-180924/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			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-2024-43756**	hotoshop/apsb24-72.html	
Out-of-bounds Write	13-Sep-2024	7.8	Photoshop Desktop versions 24.7.4, 25.11 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-2024-43760**	https://helpx.adobe.com/security/products/photoshop/apsb24-72.html	A-ADO-PHOT-180924/54
Out-of-bounds Write	13-Sep-2024	7.8	Photoshop Desktop versions 24.7.4, 25.11 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the	https://helpx.adobe.com/security/products/photoshop/apsb24-72.html	A-ADO-PHOT-180924/55

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
			context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-45108**		
Out-of-bounds Write	13-Sep-2024	7.8	Photoshop Desktop versions 24.7.4, 25.11 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-2024-45109**	https://helpx.adobe.com/security/products/photoshop/apsb24-72.html	A-ADO-PHOT-180924/56
Product: premiere_pro					
Affected Version(s): * Up to (excluding) 23.6.9					
Out-of-bounds Write	13-Sep-2024	7.8	Premiere Pro versions 24.5, 23.6.8 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	https://helpx.adobe.com/security/products/premiere_pro/apsb24-58.html	A-ADO-PREM-180924/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39384**		
Use After Free	13-Sep-2024	5.5	Premiere Pro versions 24.5, 23.6.8 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39385**	https://helpx.adobe.com/security/products/premiere_pro/apsb24-58.html	A-ADO-PREM-180924/58
Affected Version(s): From (including) 24.0 Up to (excluding) 24.6					
Out-of-bounds Write	13-Sep-2024	7.8	Premiere Pro versions 24.5, 23.6.8 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/premiere_pro/apsb24-58.html	A-ADO-PREM-180924/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID: CVE-2024-39384**		
Use After Free	13-Sep-2024	5.5	Premiere Pro versions 24.5, 23.6.8 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39385**	https://helpx.adobe.com/security/products/premiere_pro/apsb24-58.html	A-ADO-PREM-180924/60
Vendor: alwindoss					
Product: akademy					
Affected Version(s): * Up to (including) 2024-08-24					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Sep-2024	5.4	A vulnerability was found in alwindoss akademy up to 35caccea888ed63d5489e211c99edff1f62efdba. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file cmd/akademy/han	N/A	A-ALW-AKAD-180924/61

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
			dler/handlers.go. The manipulation of the argument emailAddress leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. **CVE ID: CVE-2024-8407**		
Vendor: angeljudesuarez					
Product: event_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Sep-2024	9.8	Sourcecodehero Event Management System1.0 is vulnerable to SQL Injection via the parameter 'username' in /event/admin/login.php. **CVE ID: CVE-2024-44727**	N/A	A-ANG-EVEN-180924/62
Improper Neutralization of Input During Web Page Generation	05-Sep-2024	6.1	Sourcecodehero Event Management System 1.0 allows Stored Cross-Site Scripting via parameters Full Name, Address, Email, and contact#	N/A	A-ANG-EVEN-180924/63

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
('Cross-site Scripting')			in /clientdetails/admin/regester.php. **CVE ID: CVE-2024-44728**		
Product: tailoring_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Sep-2024	9.8	A vulnerability was found in itsourcecode Tailoring Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /inccatadd.php. The manipulation of the argument title 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-2024-8570**	N/A	A-ANG-TAIL-180924/64
Vendor: ankitpokhrel					
Product: dynamic_featured_image					
Affected Version(s): * Up to (including) 3.7.0					
Improper Neutralization of Input During Web Page Generation	05-Sep-2024	5.4	The Dynamic Featured Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the	N/A	A-ANK-DYNA-180924/65

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
('Cross-site Scripting')			'dfiFeatured' parameter in all versions up to, and including, 3.7.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-6929**		
Vendor: anujk305					
Product: bus_pass_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Sep-2024	4.8	phpgurukul Bus Pass Management System 1.0 is vulnerable to Cross-site scripting (XSS) in /admin/pass-bwdates-reports-details.php via fromdate and todate parameters. **CVE ID: CVE-2024-44798**	N/A	A-ANU-BUS_-180924/66
Vendor: Apache					
Product: ofbiz					
Affected Version(s): * Up to (excluding) 18.12.16					

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
Server-Side Request Forgery (SSRF)	04-Sep-2024	9.8	Server-Side Request Forgery (SSRF), Improper Control of Generation of Code ('Code Injection') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 18.12.16. Users are recommended to upgrade to version 18.12.16, which fixes the issue. **CVE ID: CVE-2024-45507**	https://issues.apache.org/jira/browse/OFBIZ-13132, https://ofbiz.apache.org/security.html	A-APA-OFBI-180924/67
Direct Request ('Forced Browsing')	04-Sep-2024	7.5	Direct Request ('Forced Browsing') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 18.12.16. Users are recommended to upgrade to version 18.12.16, which fixes the issue. **CVE ID: CVE-2024-45195**	https://issues.apache.org/jira/browse/OFBIZ-13130, https://lists.apache.org/thread/o90dd9lbk1hh3t2557t2y2qvrh92p7wy, https://ofbiz.apache.org/security.html	A-APA-OFBI-180924/68
Vendor: ARM					
Product: mbed_tls					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 2.26.0 Up to (excluding) 2.28.9					
N/A	05-Sep-2024	5.1	An issue was discovered in Mbed TLS before 2.28.9 and 3.x before 3.6.1, in which the user-selected algorithm is not used. Unlike previously documented, enabling MBEDTLS_PSA_HMAC_DRBG_MD_TYPE does not cause the PSA subsystem to use HMAC_DRBG: it uses HMAC_DRBG only when MBEDTLS_PSA_CRYPTO_EXTERNAL_RNG and MBEDTLS_CTR_DRBG_C are disabled. **CVE ID: CVE-2024-45157**	https://mbed-tls.readthedocs.io/en/latest/security-advisories/, https://mbed-tls.readthedocs.io/en/latest/security-advisories/mbedtls-security-advisory-2024-08-1/	A-ARM-MBED-180924/69
Affected Version(s): From (including) 3.2.0 Up to (excluding) 3.6.1					
N/A	05-Sep-2024	5.1	An issue was discovered in Mbed TLS before 2.28.9 and 3.x before 3.6.1, in which the user-selected algorithm is not used. Unlike previously documented, enabling MBEDTLS_PSA_HMAC_DRBG_MD_TYPE does not cause the PSA subsystem to use HMAC_DRBG: it	https://mbed-tls.readthedocs.io/en/latest/security-advisories/, https://mbed-tls.readthedocs.io/en/latest/security-advisories/mbedtls-security-advisory-2024-08-1/	A-ARM-MBED-180924/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uses HMAC_DRBG only when MBEDTLS_PSA_CRYPTO_EXTERNAL_RNG and MBEDTLS_CTR_DRBG_C are disabled. **CVE ID: CVE-2024-45157**		
Product: trusted_firmware-m					
Affected Version(s): * Up to (including) 2.0.0					
N/A	05-Sep-2024	4.7	An issue was discovered in Trusted Firmware-M through 2.0.0. The lack of argument verification in the logging subsystem allows attackers to read sensitive data via the login function. **CVE ID: CVE-2023-51712**	https://trustedfirmware-m.readthedocs.io/en/latest/security/security_advisories/debug_log_vulnerability.html	A-ARM-TRUS-180924/71
Vendor: audiobookshelf					
Product: audiobookshelf					
Affected Version(s): * Up to (excluding) 2.13.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Sep-2024	4.3	audiobookshelf is a self-hosted audiobook and podcast server. A non-admin user is not allowed to create libraries (or access only the ones they have permission to). However, the `LibraryController` is missing the check	https://github.com/advplyr/audiobookshelf/security/advisories/GHSA-gg56-vj58-g5mc	A-AUD-AUDI-180924/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for admin user and thus allows a path traversal issue. Allowing non-admin users to write to any directory in the system can be seen as a form of path traversal. However, since it can be restricted to only admin permissions, fixing this is relatively simple and falls more into the realm of Role-Based Access Control (RBAC). This issue has been addressed in release version 2.13.0. All users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2024-43797**		
Vendor: bitapps					
Product: file_manager					
Affected Version(s): From (including) 6.0 Up to (excluding) 6.5.6					
Concurrent Execution using Shared Resource with Improper Synchronization	05-Sep-2024	8.1	The Bit File Manager plugin for WordPress is vulnerable to Remote Code Execution in versions 6.0 to 6.5.5 via the 'checkSyntax'	https://plugins.trac.wordpress.org/changeset/3138710/	A-BIT-FILE-180924/73

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			function. This is due to writing a temporary file to a publicly accessible directory before performing file validation. This makes it possible for unauthenticated attackers to execute code on the server if an administrator has allowed Guest User read permissions. **CVE ID: CVE-2024-7627**		
Vendor: blakeembrey					
Product: template					
Affected Version(s): * Up to (excluding) 1.2.0					
Improper Control of Generation of Code ('Code Injection')	03-Sep-2024	9.8	@blakeembrey/template is a string template library. Prior to version 1.2.0, it is possible to inject and run code within the template if the attacker has access to write the template name. Version 1.2.0 contains a patch. As a workaround, don't pass untrusted input as the template display name, or don't use the display name feature.	https://github.com/blakeembrey/js-template/commit/b8d9aa999e464816c6cfb14acd1ad0f5d1e335aa, https://github.com/blakeembrey/js-template/security/advisories/GHSA-q765-wm9j-66qj	A-BLA-TEMP-180924/74

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
			CVE ID: CVE-2024-45390		
Vendor: checkmk					
Product: checkmk					
Affected Version(s): * Up to (excluding) 2.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-2024	6.1	Improper neutralization of input in Checkmk before version 2.3.0p14 allows attackers to inject and run malicious scripts in the Robotmk logs view. **CVE ID: CVE-2024-38858**	https://checkmk.com/werk/17232	A-CHE-CHEC-180924/75
Affected Version(s): 2.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-2024	6.1	Improper neutralization of input in Checkmk before version 2.3.0p14 allows attackers to inject and run malicious scripts in the Robotmk logs view. **CVE ID: CVE-2024-38858**	https://checkmk.com/werk/17232	A-CHE-CHEC-180924/76
Vendor: Cisco					
Product: duo_authentication_for_epic					
Affected Version(s): 1.0.0					
Missing Encryption of Sensitive Data	04-Sep-2024	5.5	A vulnerability in Cisco Duo Epic for Hyperdrive could allow an authenticated, local attacker to view sensitive information in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-epic-info-sdLv6h8y	A-CIS-DUO_-180924/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cleartext on an affected system. This vulnerability is due to improper storage of an unencrypted registry key. A low-privileged attacker could exploit this vulnerability by viewing or querying the registry key on the affected system. A successful exploit could allow the attacker to view sensitive information in cleartext. **CVE ID: CVE-2024-20503**		
Affected Version(s): 1.0.1					
Missing Encryption of Sensitive Data	04-Sep-2024	5.5	A vulnerability in Cisco Duo Epic for Hyperdrive could allow an authenticated, local attacker to view sensitive information in cleartext on an affected system. This vulnerability is due to improper storage of an unencrypted registry key. A low-privileged attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-epic-info-sdLv6h8y	A-CIS-DUO_-180924/78

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
			vulnerability by viewing or querying the registry key on the affected system. A successful exploit could allow the attacker to view sensitive information in cleartext. **CVE ID: CVE-2024-20503**		
Affected Version(s): 1.1.10					
Missing Encryption of Sensitive Data	04-Sep-2024	5.5	A vulnerability in Cisco Duo Epic for Hyperdrive could allow an authenticated, local attacker to view sensitive information in cleartext on an affected system. This vulnerability is due to improper storage of an unencrypted registry key. A low-privileged attacker could exploit this vulnerability by viewing or querying the registry key on the affected system. A successful exploit could allow the attacker to view sensitive	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-epic-info-sdLv6h8y	A-CIS-DUO_-180924/79

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
			information in cleartext. **CVE ID: CVE-2024-20503**		
Affected Version(s): 1.1.13					
Missing Encryption of Sensitive Data	04-Sep-2024	5.5	A vulnerability in Cisco Duo Epic for Hyperdrive could allow an authenticated, local attacker to view sensitive information in cleartext on an affected system. This vulnerability is due to improper storage of an unencrypted registry key. A low-privileged attacker could exploit this vulnerability by viewing or querying the registry key on the affected system. A successful exploit could allow the attacker to view sensitive information in cleartext. **CVE ID: CVE-2024-20503**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-epic-info-sdLv6h8y	A-CIS-DUO_-180924/80
Affected Version(s): 1.1.9					
Missing Encryption of Sensitive Data	04-Sep-2024	5.5	A vulnerability in Cisco Duo Epic for Hyperdrive could allow an	https://sec.cloudapps.cisco.com/security/center/content/Cisco	A-CIS-DUO_-180924/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to view sensitive information in cleartext on an affected system. This vulnerability is due to improper storage of an unencrypted registry key. A low-privileged attacker could exploit this vulnerability by viewing or querying the registry key on the affected system. A successful exploit could allow the attacker to view sensitive information in cleartext. **CVE ID: CVE-2024-20503**	SecurityAdvisory/cisco-sa-duo-epic-info-sdLv6h8y	
Affected Version(s): 1.2.0.95					
Missing Encryption of Sensitive Data	04-Sep-2024	5.5	A vulnerability in Cisco Duo Epic for Hyperdrive could allow an authenticated, local attacker to view sensitive information in cleartext on an affected system. This vulnerability is due to improper storage of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-epic-info-sdLv6h8y	A-CIS-DUO_-180924/82

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
			unencrypted registry key. A low-privileged attacker could exploit this vulnerability by viewing or querying the registry key on the affected system. A successful exploit could allow the attacker to view sensitive information in cleartext. **CVE ID: CVE-2024-20503**		
Product: smart_license_utility					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.3.0					
Use of Hard-coded Credentials	04-Sep-2024	9.8	A vulnerability in Cisco Smart Licensing Utility could allow an unauthenticated, remote attacker to log in to an affected system by using a static administrative credential. This vulnerability is due to an undocumented static user credential for an administrative account. An attacker could exploit this vulnerability by using the static	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw	A-CIS-SMAR-180924/83

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
			credentials to log in to the affected system. A successful exploit could allow the attacker to log in to the affected system with administrative privileges over the API of the Cisco Smart Licensing Utility application. **CVE ID: CVE-2024-20439**		
Vendor: Clamav					
Product: clamav					
Affected Version(s): * Up to (excluding) 0.103.12					
Out-of-bounds Read	04-Sep-2024	7.5	A vulnerability in the PDF parsing module of Clam AntiVirus (ClamAV) versions 1.4.0, 1.3.2 and prior versions, all 1.2.x versions, 1.0.6 and prior versions, all 0.105.x versions, all 0.104.x versions, and 0.103.11 and all prior versions could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to an out of bounds read. An attacker could	https://blog.clamav.net/2024/09/clamav-141-132-107-and-010312-security.html	A-CLA-CLAM-180924/84

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
			exploit this vulnerability by submitting a crafted PDF file to be scanned by ClamAV on an affected device. An exploit could allow the attacker to terminate the scanning process. **CVE ID: CVE-2024-20505**		
Improper Check for Unusual or Exceptional Conditions	04-Sep-2024	6.1	A vulnerability in the ClamD service module of Clam AntiVirus (ClamAV) versions 1.4.0, 1.3.2 and prior versions, all 1.2.x versions, 1.0.6 and prior versions, all 0.105.x versions, all 0.104.x versions, and 0.103.11 and all prior versions could allow an authenticated, local attacker to corrupt critical system files. The vulnerability is due to allowing the ClamD process to write to its log file while privileged without checking if the logfile has been replaced with a symbolic link. An attacker could exploit this vulnerability if they	N/A	A-CLA-CLAM-180924/85

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			replace the ClamD log file with a symlink to a critical system file and then find a way to restart the ClamD process. An exploit could allow the attacker to corrupt a critical system file by appending ClamD log messages after restart. **CVE ID: CVE-2024-20506**		
Affected Version(s): 1.4.0					
Out-of-bounds Read	04-Sep-2024	7.5	A vulnerability in the PDF parsing module of Clam AntiVirus (ClamAV) versions 1.4.0, 1.3.2 and prior versions, all 1.2.x versions, 1.0.6 and prior versions, all 0.105.x versions, all 0.104.x versions, and 0.103.11 and all prior versions could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to an out of bounds read. An attacker could	https://blog.clamav.net/2024/09/clamav-141-132-107-and-010312-security.html	A-CLA-CLAM-180924/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by submitting a crafted PDF file to be scanned by ClamAV on an affected device. An exploit could allow the attacker to terminate the scanning process. **CVE ID: CVE-2024-20505**		
Improper Check for Unusual or Exceptional Conditions	04-Sep-2024	6.1	A vulnerability in the ClamD service module of Clam AntiVirus (ClamAV) versions 1.4.0, 1.3.2 and prior versions, all 1.2.x versions, 1.0.6 and prior versions, all 0.105.x versions, all 0.104.x versions, and 0.103.11 and all prior versions could allow an authenticated, local attacker to corrupt critical system files. The vulnerability is due to allowing the ClamD process to write to its log file while privileged without checking if the logfile has been replaced with a symbolic link. An attacker could exploit this vulnerability if they	N/A	A-CLA-CLAM-180924/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			replace the ClamD log file with a symlink to a critical system file and then find a way to restart the ClamD process. An exploit could allow the attacker to corrupt a critical system file by appending ClamD log messages after restart. **CVE ID: CVE-2024-20506**		
Affected Version(s): From (including) 0.104.0 Up to (excluding) 1.0.7					
Out-of-bounds Read	04-Sep-2024	7.5	A vulnerability in the PDF parsing module of Clam AntiVirus (ClamAV) versions 1.4.0, 1.3.2 and prior versions, all 1.2.x versions, 1.0.6 and prior versions, all 0.105.x versions, all 0.104.x versions, and 0.103.11 and all prior versions could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to an out of bounds read. An attacker could	https://blog.clamav.net/2024/09/clamav-141-132-107-and-010312-security.html	A-CLA-CLAM-180924/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by submitting a crafted PDF file to be scanned by ClamAV on an affected device. An exploit could allow the attacker to terminate the scanning process. **CVE ID: CVE-2024-20505**		
Improper Check for Unusual or Exceptional Conditions	04-Sep-2024	6.1	A vulnerability in the ClamD service module of Clam AntiVirus (ClamAV) versions 1.4.0, 1.3.2 and prior versions, all 1.2.x versions, 1.0.6 and prior versions, all 0.105.x versions, all 0.104.x versions, and 0.103.11 and all prior versions could allow an authenticated, local attacker to corrupt critical system files. The vulnerability is due to allowing the ClamD process to write to its log file while privileged without checking if the logfile has been replaced with a symbolic link. An attacker could exploit this vulnerability if they	N/A	A-CLA-CLAM-180924/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			replace the ClamD log file with a symlink to a critical system file and then find a way to restart the ClamD process. An exploit could allow the attacker to corrupt a critical system file by appending ClamD log messages after restart. **CVE ID: CVE-2024-20506**		
Affected Version(s): From (including) 1.2.0 Up to (excluding) 1.3.2					
Out-of-bounds Read	04-Sep-2024	7.5	A vulnerability in the PDF parsing module of Clam AntiVirus (ClamAV) versions 1.4.0, 1.3.2 and prior versions, all 1.2.x versions, 1.0.6 and prior versions, all 0.105.x versions, all 0.104.x versions, and 0.103.11 and all prior versions could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to an out of bounds read. An attacker could	https://blog.clamav.net/2024/09/clamav-141-132-107-and-010312-security.html	A-CLA-CLAM-180924/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by submitting a crafted PDF file to be scanned by ClamAV on an affected device. An exploit could allow the attacker to terminate the scanning process. **CVE ID: CVE-2024-20505**		
Improper Check for Unusual or Exceptional Conditions	04-Sep-2024	6.1	A vulnerability in the ClamD service module of Clam AntiVirus (ClamAV) versions 1.4.0, 1.3.2 and prior versions, all 1.2.x versions, 1.0.6 and prior versions, all 0.105.x versions, all 0.104.x versions, and 0.103.11 and all prior versions could allow an authenticated, local attacker to corrupt critical system files. The vulnerability is due to allowing the ClamD process to write to its log file while privileged without checking if the logfile has been replaced with a symbolic link. An attacker could exploit this vulnerability if they	N/A	A-CLA-CLAM-180924/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			replace the ClamD log file with a symlink to a critical system file and then find a way to restart the ClamD process. An exploit could allow the attacker to corrupt a critical system file by appending ClamD log messages after restart. **CVE ID: CVE-2024-20506**		
Vendor: cloudcannon					
Product: pagefinder					
Affected Version(s): * Up to (excluding) 1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	5.4	Pagefind, a fully static search library, initializes its dynamic JavaScript and WebAssembly files relative to the location of the first script the user loads. This information is gathered by looking up the value of `document.currentScript.src`. Prior to Pagefind version 1.1.1, it is possible to "clobber" this lookup with otherwise benign HTML on the page. This will cause `document.current	https://github.com/CloudCannon/pagefind/commit/14ec96864eabaf1d7d809d5da0186a8856261eeb, https://github.com/CloudCannon/pagefind/security/advisories/GHSA-gprj-6m2f-j9hx	A-CLO-PAGE-180924/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Script.src` to resolve as an external domain, which will then be used by Pagefind to load dependencies. This exploit would only work in the case that an attacker could inject HTML to a live, hosted, website. In these cases, this would act as a way to escalate the privilege available to an attacker. This assumes they have the ability to add some elements to the page (for example, `img` tags with a `name` attribute), but not others, as adding a `script` to the page would itself be the cross-site scripting vector. Pagefind has tightened this resolution in version 1.1.1 by ensuring the source is loaded from a valid script element. There are no reports of this being exploited in the wild via Pagefind. **CVE ID: CVE-2024-45389**		

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
Vendor: code-projects					
Product: crud_operation_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Sep-2024	9.8	A vulnerability was found in code-projects Crud Operation System 1.0. It has been classified as critical. This affects an unknown part of the file /updatedata.php. The manipulation of the argument sid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8762**	N/A	A-COD-CRUD-180924/93
Product: inventory_management					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	8.8	A vulnerability classified as critical was found in code-projects Inventory Management 1.0. Affected by this vulnerability is an unknown functionality of the file /model/viewProduct.php of the component Products Table	N/A	A-COD-INVE-180924/94

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
			Page. 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-2024-8710**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Sep-2024	5.4	A vulnerability classified as problematic was found in code-projects Inventory Management 1.0. This vulnerability affects unknown code of the file /view/registration.php of the component Registration Form. The manipulation with the input <script>alert(1)</script> leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8605**	N/A	A-COD-INVE-180924/95
Vendor: containers					
Product: aardvark-dns					
Affected Version(s): 1.12.0					

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
N/A	04-Sep-2024	7.5	A flaw was found in Aardvark-dns versions 1.12.0 and 1.12.1. They contain a denial of service vulnerability due to serial processing of TCP DNS queries. This flaw allows a malicious client to keep a TCP connection open indefinitely, causing other DNS queries to time out and resulting in a denial of service for all other containers using aardvark-dns. **CVE ID: CVE-2024-8418**	N/A	A-CON-AARD-180924/96
Affected Version(s): 1.12.1					
N/A	04-Sep-2024	7.5	A flaw was found in Aardvark-dns versions 1.12.0 and 1.12.1. They contain a denial of service vulnerability due to serial processing of TCP DNS queries. This flaw allows a malicious client to keep a TCP connection open indefinitely, causing other DNS queries to time out and resulting in a denial of service for all other containers	N/A	A-CON-AARD-180924/97

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
			using aardvark-dns. **CVE ID: CVE-2024-8418**		
Vendor: Craftcms					
Product: craft_cms					
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Sep-2024	4.8	Craft is a content management system (CMS). Craft CMS 5 stored XSS can be triggered by the breadcrumb list and title fields with user input. **CVE ID: CVE-2024-45406**	https://github.com/craftcms/cms/commit/b7348942f8131b3868ec6f46d615baae50151bb8, https://github.com/craftcms/cms/security/advisories/GHSA-28h4-788g-rh42	A-CRA-CRAF-180924/98
Vendor: dataflowx					
Product: datadiodex					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.1.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	7.5	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in DataFlowX Technology DataDiodeX allows Path Traversal.This issue affects DataDiodeX: from v3.0.0 before v3.1.7. **CVE ID: CVE-2024-6445**	N/A	A-DAT-DATA-180924/99
Vendor: deathbreak					

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
Product: drug					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability in the component \bean\Manager.java of Drug v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the user parameter. **CVE ID: CVE-2024-44837**	N/A	A-DEA-DRUG-180924/100
Vendor: Dell					
Product: insightiq					
Affected Version(s): 5.0					
Use of Hard-coded Credentials	10-Sep-2024	4.4	Dell PowerScale InsightIQ, version 5.0, contain a Use of hard coded Credentials vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure. **CVE ID: CVE-2024-39582**	https://www.dell.com/support/kbdoc/en-us/000228412/dsa-2024-360-security-update-for-dell-powerscale-insightiq-for-multiple-security-vulnerabilities	A-DEL-INSI-180924/101
Affected Version(s): 5.1.0					
N/A	10-Sep-2024	4.4	Dell PowerScale InsightIQ, version 5.1, contain an	https://www.dell.com/support/kbdoc/en-	A-DEL-INSI-180924/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Improper Privilege Management vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Denial of service. **CVE ID: CVE-2024-39574**	us/000228412/dsa-2024-360-security-update-for-dell-powerscale-insightiq-for-multiple-security-vulnerabilities	
Affected Version(s): From (including) 5.0 Up to (excluding) 5.1.1					
Files or Directories Accessible to External Parties	10-Sep-2024	9.8	Dell PowerScale InsightIQ, versions 5.0 through 5.1, contains a File or Directories Accessible to External Parties vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability to read, modify, and delete arbitrary files. **CVE ID: CVE-2024-39581**	https://www.dell.com/support/kbdoc/en-us/000228412/dsa-2024-360-security-update-for-dell-powerscale-insightiq-for-multiple-security-vulnerabilities	A-DEL-INSI-180924/103
Use of a Broken or Risky Cryptographic Algorithm	10-Sep-2024	9.8	Dell PowerScale InsightIQ, versions 5.0 through 5.1, contains a Use of a Broken or Risky Cryptographic Algorithm vulnerability. An unauthenticated attacker with	https://www.dell.com/support/kbdoc/en-us/000228412/dsa-2024-360-security-update-for-dell-powerscale-insightiq-for-multiple-	A-DEL-INSI-180924/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote access could potentially exploit this vulnerability, leading to Elevation of privileges. **CVE ID: CVE-2024-39583**	security-vulnerabilities	
N/A	10-Sep-2024	6.7	Dell PowerScale InsightIQ, versions 5.0 through 5.1, contains an Improper Access Control vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges. **CVE ID: CVE-2024-39580**	https://www.dell.com/support/kbdoc/en-us/000228412/dsa-2024-360-security-update-for-dell-powerscale-insightiq-for-multiple-security-vulnerabilities	A-DEL-INSI-180924/105
Product: path_to_powerprotect					
Affected Version(s): 1.1					
N/A	03-Sep-2024	4.9	Dell Path to PowerProtect, versions 1.1, 1.2, contains an Exposure of Private Personal Information to an Unauthorized Actor vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to	https://www.dell.com/support/kbdoc/en-us/000227430/dsa-2024-291-security-update-for-dell-path-to-powerprotect-for-security-vulnerability	A-DEL-PATH-180924/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information exposure. **CVE ID: CVE-2024-37136**		
Affected Version(s): 1.2					
N/A	03-Sep-2024	4.9	Dell Path to PowerProtect, versions 1.1, 1.2, contains an Exposure of Private Personal Information to an Unauthorized Actor vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to information exposure. **CVE ID: CVE-2024-37136**	https://www.dell.com/support/kbdoc/en-us/000227430/dsa-2024-291-security-update-for-dell-path-to-powerprotect-for-security-vulnerability	A-DEL-PATH-180924/107
Vendor: dfinity					
Product: canister_developer_kit_for_the_internet_computer					
Affected Version(s): 0.10.0					
Missing Release of Memory after Effective Lifetime	05-Sep-2024	7.5	When a canister method is called via ic_cdk::call* , a new Future CallFuture is created and can be awaited by the caller to get the execution result. Internally, the state of the Future is tracked and stored in a struct called CallFutureState. A	https://github.com/dfinity/cdk-rs/pull/509	A-DFI-CANI-180924/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bug in the polling implementation of the CallFuture allows multiple references to be held for this internal state and not all references were dropped before the Future is resolved. Since we have unaccounted references held, a copy of the internal state ended up being persisted in the canister's heap and thus causing a memory leak. Impact Canisters built in Rust with ic_cdk and ic_cdk_timers are affected. If these canisters call a canister method, use timers or heartbeat, they will likely leak a small amount of memory on every such operation. In the worst case, this could lead to heap memory exhaustion triggered by an attacker. Motoko based canisters are not affected by the bug. PatchesThe patch has been		

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
			backported to all minor versions between >= 0.8.0, <= 0.15.0. The patched versions available are 0.8.2, 0.9.3, 0.10.1, 0.11.6, 0.12.2, 0.13.5, 0.14.1, 0.15.1 and their previous versions have been yanked. WorkaroundsThere are no known workarounds at the moment. Developers are recommended to upgrade their canister as soon as possible to the latest available patched version of ic_cdk to avoid running out of Wasm heap memory. Upgrading the canisters (without updating `ic_cdk`) also frees the leaked memory but it's only a temporary solution. **CVE ID: CVE-2024-7884**		
Affected Version(s): 0.14.0					
Missing Release of Memory after	05-Sep-2024	7.5	When a canister method is called via ic_cdk::call* , a new Future CallFuture is	https://github.com/dfinity/cdk-rs/pull/509	A-DFI-CANI-180924/109

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
Effective Lifetime			created and can be awaited by the caller to get the execution result. Internally, the state of the Future is tracked and stored in a struct called CallFutureState. A bug in the polling implementation of the CallFuture allows multiple references to be held for this internal state and not all references were dropped before the Future is resolved. Since we have unaccounted references held, a copy of the internal state ended up being persisted in the canister's heap and thus causing a memory leak. Impact Canisters built in Rust with ic_cdk and ic_cdk_timers are affected. If these canisters call a canister method, use timers or heartbeat, they will likely leak a small amount of memory on every such operation. In the worst case, this could lead to heap memory		

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
			exhaustion triggered by an attacker. Motoko based canisters are not affected by the bug. PatchesThe patch has been backported to all minor versions between >= 0.8.0, <= 0.15.0. The patched versions available are 0.8.2, 0.9.3, 0.10.1, 0.11.6, 0.12.2, 0.13.5, 0.14.1, 0.15.1 and their previous versions have been yanked. WorkaroundsThere are no known workarounds at the moment. Developers are recommended to upgrade their canister as soon as possible to the latest available patched version of ic_cdk to avoid running out of Wasm heap memory. Upgrading the canisters (without updating `ic_cdk`) also frees the leaked memory but it's only a temporary solution.		

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
			CVE ID: CVE-2024-7884		
Affected Version(s): 0.15.0					
Missing Release of Memory after Effective Lifetime	05-Sep-2024	7.5	When a canister method is called via ic_cdk::call* , a new Future CallFuture is created and can be awaited by the caller to get the execution result. Internally, the state of the Future is tracked and stored in a struct called CallFutureState. A bug in the polling implementation of the CallFuture allows multiple references to be held for this internal state and not all references were dropped before the Future is resolved. Since we have unaccounted references held, a copy of the internal state ended up being persisted in the canister's heap and thus causing a memory leak. Impact Canisters built in Rust with ic_cdk and ic_cdk_timers are affected. If these canisters call a canister method,	https://github.com/dfinity/cdk-rs/pull/509	A-DFI-CANI-180924/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use timers or heartbeat, they will likely leak a small amount of memory on every such operation. In the worst case, this could lead to heap memory exhaustion triggered by an attacker. Motoko based canisters are not affected by the bug. PatchesThe patch has been backported to all minor versions between >= 0.8.0, <= 0.15.0. The patched versions available are 0.8.2, 0.9.3, 0.10.1, 0.11.6, 0.12.2, 0.13.5, 0.14.1, 0.15.1 and their previous versions have been yanked. WorkaroundsThere are no known workarounds at the moment. Developers are recommended to upgrade their canister as soon as possible to the latest available patched version of ic_cdk to avoid running out of		

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
			Wasm heap memory. Upgrading the canisters (without updating `ic_cdk`) also frees the leaked memory but it's only a temporary solution. **CVE ID: CVE-2024-7884**		
Affected Version(s): From (including) 0.11.0 Up to (excluding) 0.11.6					
Missing Release of Memory after Effective Lifetime	05-Sep-2024	7.5	When a canister method is called via ic_cdk::call* , a new Future CallFuture is created and can be awaited by the caller to get the execution result. Internally, the state of the Future is tracked and stored in a struct called CallFutureState. A bug in the polling implementation of the CallFuture allows multiple references to be held for this internal state and not all references were dropped before the Future is resolved. Since we have unaccounted references held, a copy of the internal state ended up being persisted in	https://github.com/dfinity/cdk-rs/pull/509	A-DFI-CANI-180924/111

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 versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the canister's heap and thus causing a memory leak. Impact Canisters built in Rust with ic_cdk and ic_cdk_timers are affected. If these canisters call a canister method, use timers or heartbeat, they will likely leak a small amount of memory on every such operation. In the worst case, this could lead to heap memory exhaustion triggered by an attacker. Motoko based canisters are not affected by the bug. PatchesThe patch has been backported to all minor versions between >= 0.8.0, <= 0.15.0. The patched versions available are 0.8.2, 0.9.3, 0.10.1, 0.11.6, 0.12.2, 0.13.5, 0.14.1, 0.15.1 and their previous versions have been yanked. WorkaroundsThere are no known workarounds at the moment.		

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
			Developers are recommended to upgrade their canister as soon as possible to the latest available patched version of ic_cdk to avoid running out of Wasm heap memory. Upgrading the canisters (without updating `ic_cdk`) also frees the leaked memory but it's only a temporary solution. **CVE ID: CVE-2024-7884**		
Affected Version(s): From (including) 0.12.0 Up to (excluding) 0.12.2					
Missing Release of Memory after Effective Lifetime	05-Sep-2024	7.5	When a canister method is called via ic_cdk::call* , a new Future CallFuture is created and can be awaited by the caller to get the execution result. Internally, the state of the Future is tracked and stored in a struct called CallFutureState. A bug in the polling implementation of the CallFuture allows multiple references to be held for this internal state and	https://github.com/dfinity/cdk-rs/pull/509	A-DFI-CANI-180924/112

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
			not all references were dropped before the Future is resolved. Since we have unaccounted references held, a copy of the internal state ended up being persisted in the canister's heap and thus causing a memory leak. Impact Canisters built in Rust with ic_cdk and ic_cdk_timers are affected. If these canisters call a canister method, use timers or heartbeat, they will likely leak a small amount of memory on every such operation. In the worst case, this could lead to heap memory exhaustion triggered by an attacker. Motoko based canisters are not affected by the bug. PatchesThe patch has been backported to all minor versions between >= 0.8.0, <= 0.15.0. The patched versions available are 0.8.2, 0.9.3, 0.10.1, 0.11.6,		

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
			0.12.2, 0.13.5, 0.14.1, 0.15.1 and their previous versions have been yanked. WorkaroundsThere are no known workarounds at the moment. Developers are recommended to upgrade their canister as soon as possible to the latest available patched version of ic_cdk to avoid running out of Wasm heap memory. Upgrading the canisters (without updating `ic_cdk`) also frees the leaked memory but it's only a temporary solution. **CVE ID: CVE-2024-7884**		
Affected Version(s): From (including) 0.13.0 Up to (excluding) 0.13.5					
Missing Release of Memory after Effective Lifetime	05-Sep-2024	7.5	When a canister method is called via ic_cdk::call* , a new Future CallFuture is created and can be awaited by the caller to get the execution result. Internally, the state of the Future is tracked and stored	https://github.com/dfinity/cdk-rs/pull/509	A-DFI-CANI-180924/113

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
			in a struct called CallFutureState. A bug in the polling implementation of the CallFuture allows multiple references to be held for this internal state and not all references were dropped before the Future is resolved. Since we have unaccounted references held, a copy of the internal state ended up being persisted in the canister's heap and thus causing a memory leak. Impact Canisters built in Rust with ic_cdk and ic_cdk_timers are affected. If these canisters call a canister method, use timers or heartbeat, they will likely leak a small amount of memory on every such operation. In the worst case, this could lead to heap memory exhaustion triggered by an attacker. Motoko based canisters are not affected by the bug.		

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
			PatchesThe patch has been backported to all minor versions between >= 0.8.0, <= 0.15.0. The patched versions available are 0.8.2, 0.9.3, 0.10.1, 0.11.6, 0.12.2, 0.13.5, 0.14.1, 0.15.1 and their previous versions have been yanked. WorkaroundsThere are no known workarounds at the moment. Developers are recommended to upgrade their canister as soon as possible to the latest available patched version of ic_cdk to avoid running out of Wasm heap memory. Upgrading the canisters (without updating `ic_cdk`) also frees the leaked memory but it's only a temporary solution. **CVE ID: CVE-2024-7884**		
Affected Version(s): From (including) 0.8.0 Up to (excluding) 0.8.2					

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
Missing Release of Memory after Effective Lifetime	05-Sep-2024	7.5	When a canister method is called via ic_cdk::call* , a new Future CallFuture is created and can be awaited by the caller to get the execution result. Internally, the state of the Future is tracked and stored in a struct called CallFutureState. A bug in the polling implementation of the CallFuture allows multiple references to be held for this internal state and not all references were dropped before the Future is resolved. Since we have unaccounted references held, a copy of the internal state ended up being persisted in the canister's heap and thus causing a memory leak. Impact Canisters built in Rust with ic_cdk and ic_cdk_timers are affected. If these canisters call a canister method, use timers or heartbeat, they will likely leak a small amount of memory	https://github.com/dfinity/cdk-rs/pull/509	A-DFI-CANI-180924/114

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
			on every such operation. In the worst case, this could lead to heap memory exhaustion triggered by an attacker. Motoko based canisters are not affected by the bug. PatchesThe patch has been backported to all minor versions between >= 0.8.0, <= 0.15.0. The patched versions available are 0.8.2, 0.9.3, 0.10.1, 0.11.6, 0.12.2, 0.13.5, 0.14.1, 0.15.1 and their previous versions have been yanked. WorkaroundsThere are no known workarounds at the moment. Developers are recommended to upgrade their canister as soon as possible to the latest available patched version of ic_cdk to avoid running out of Wasm heap memory. Upgrading the canisters (without updating `ic_cdk`)		

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
			also frees the leaked memory but it's only a temporary solution. **CVE ID: CVE-2024-7884**		
Affected Version(s): From (including) 0.9.0 Up to (excluding) 0.9.3					
Missing Release of Memory after Effective Lifetime	05-Sep-2024	7.5	When a canister method is called via ic_cdk::call* , a new Future CallFuture is created and can be awaited by the caller to get the execution result. Internally, the state of the Future is tracked and stored in a struct called CallFutureState. A bug in the polling implementation of the CallFuture allows multiple references to be held for this internal state and not all references were dropped before the Future is resolved. Since we have unaccounted references held, a copy of the internal state ended up being persisted in the canister's heap and thus causing a memory leak. Impact Canisters built in Rust with	https://github.com/dfinity/cdk-rs/pull/509	A-DFI-CANI-180924/115

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
			ic_cdk and ic_cdk_timers are affected. If these canisters call a canister method, use timers or heartbeat, they will likely leak a small amount of memory on every such operation. In the worst case, this could lead to heap memory exhaustion triggered by an attacker. Motoko based canisters are not affected by the bug. PatchesThe patch has been backported to all minor versions between >= 0.8.0, <= 0.15.0. The patched versions available are 0.8.2, 0.9.3, 0.10.1, 0.11.6, 0.12.2, 0.13.5, 0.14.1, 0.15.1 and their previous versions have been yanked. WorkaroundsThere are no known workarounds at the moment. Developers are recommended to upgrade their canister as soon as possible to the latest available		

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
			patched version of ic_cdk to avoid running out of Wasm heap memory. Upgrading the canisters (without updating `ic_cdk`) also frees the leaked memory but it's only a temporary solution. **CVE ID: CVE-2024-7884**		
Vendor: Docker					
Product: desktop					
Affected Version(s): * Up to (excluding) 4.34.2					
N/A	12-Sep-2024	9.8	A remote code execution (RCE) vulnerability via crafted extension description/change log could be abused by a malicious extension in Docker Desktop before 4.34.2. **CVE ID: CVE-2024-8695**	N/A	A-DOC-DESK-180924/116
N/A	12-Sep-2024	9.8	A remote code execution (RCE) vulnerability via crafted extension publisher-url/additional-urls could be abused by a malicious extension in Docker Desktop before 4.34.2.	N/A	A-DOC-DESK-180924/117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8696		
Vendor: dpgaspar					
Product: flask_app_builder					
Affected Version(s): * Up to (excluding) 4.5.1					
N/A	04-Sep-2024	5.5	Flask-AppBuilder is an application development framework. Prior to version 4.5.1, the auth DB login form default cache directives allows browser to locally store sensitive data. This can be an issue on environments using shared computer resources. Version 4.5.1 contains a patch for this issue. If upgrading is not possible, configure one's web server to send the specific HTTP headers for `/login` per the directions provided in the GitHub Security Advisory. **CVE ID: CVE-2024-45314**	https://github.com/dpgaspar/Flask-AppBuilder/commit/3030e881d2e44f4021764e18e489fe940a9b3636, https://github.com/dpgaspar/Flask-AppBuilder/security/advisories/GHSA-fw5r-6m3x-rh7p	A-DPG-FLAS-180924/118
Vendor: easytest					
Product: easytest_online_test_platform					
Affected Version(s): * Up to (including) 24e01					
Improper Neutralization of Special	02-Sep-2024	9.8	SQL Injection in download student learning course function of Easytest	N/A	A-EAS-EASY-180924/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			Online Test Platform ver.24E01 and earlier allow remote attackers to execute arbitrary SQL commands via the uid parameter. **CVE ID: CVE-2024-43772**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Sep-2024	9.8	SQL Injection in download class learning course function of Easytest Online Test Platform ver.24E01 and earlier allow remote attackers to execute arbitrary SQL commands via the cstr parameter. **CVE ID: CVE-2024-43773**	N/A	A-EAS-EASY-180924/120
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Sep-2024	8.8	SQL Injection in download personal learning course function of Easytest Online Test Platform ver.24E01 and earlier allow remote authenticated users to execute arbitrary SQL commands via the uid parameter. **CVE ID: CVE-2024-43774**	N/A	A-EAS-EASY-180924/121
Improper Neutralization of Special Elements used in an	02-Sep-2024	8.8	SQL Injection in search course titles function of Easytest Online Test Platform ver.24E01 and earlier allow	N/A	A-EAS-EASY-180924/122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			remote authenticated users to execute arbitrary SQL commands via the search parameter. **CVE ID: CVE-2024-43775**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Sep-2024	8.8	SQL Injection in mock exam function of Easytest Online Test Platform ver.24E01 and earlier allow remote authenticated users to execute arbitrary SQL commands via the qlevel parameter. **CVE ID: CVE-2024-43776**	N/A	A-EAS-EASY-180924/123
Vendor: easytest_online_test_platform_project					
Product: easytest_online_test_platform					
Affected Version(s): * Up to (including) 24e01					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Sep-2024	8.8	SQL Injection in online dictionary function of Easytest Online Test Platform ver.24E01 and earlier allow remote authenticated users to execute arbitrary SQL commands via the word parameter. **CVE ID: CVE-2024-7871**	N/A	A-EAS-EASY-180924/124
Vendor: Eclipse					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: vert.x					
Affected Version(s): From (including) 4.3.0 Up to (excluding) 4.5.10					
Allocation of Resources Without Limits or Throttling	04-Sep-2024	7.5	In Eclipse Vert.x version 4.3.0 to 4.5.9, the gRPC server does not limit the maximum length of message payload (Maven GAV: io.vertx:vertx-grpc-server and io.vertx:vertx-grpc-client). This is fixed in the 4.5.10 version. Note this does not affect the Vert.x gRPC server based grpc-java and Netty libraries (Maven GAV: io.vertx:vertx-grpc) **CVE ID: CVE-2024-8391**	https://gitlab.eclipse.org/security/cve-assignement/-/issues/31	A-ECL-VERT-180924/125
Vendor: elabftw					
Product: elabftw					
Affected Version(s): * Up to (excluding) 5.0.0					
Improper Neutralization of Input	02-Sep-2024	5.4	eLabFTW is an open source electronic lab	https://github.com/elabftw/elabftw/security/a	A-ELA-ELAB-180924/126

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
During Web Page Generation ('Cross-site Scripting')			notebook for research labs. By uploading specially crafted files, a regular user can create a circumstance where a visitor's browser runs arbitrary JavaScript code in the context of the eLabFTW application. This can be triggered by the visitor viewing a list of experiments. Viewing this allows the malicious script to act on behalf of the visitor in any way, including the creation of API keys for persistence, or other options normally available to the user. If the user viewing the page has the sysadmin role in eLabFTW, the script can act as a sysadmin (including system configuration and extensive user management roles). Users are advised to upgrade to at least version 5.0.0. There are no known workarounds for this vulnerability.	dvisories/GHSA-xp3v-w8cx-cqxc	

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
			CVE ID: CVE-2024-28100		
Vendor: Elastic					
Product: kibana					
Affected Version(s): 8.15.0					
Deserialization of Untrusted Data	09-Sep-2024	8.8	A deserialization issue in Kibana can lead to arbitrary code execution when Kibana attempts to parse a YAML document containing a crafted payload. This issue only affects users that use Elastic Security's built-in AI tools https://www.elastic.co/guide/en/security/current/ai-for-security.html and have configured an Amazon Bedrock connector https://www.elastic.co/guide/en/security/current/assistant-connect-to-bedrock.html . **CVE ID: CVE-2024-37288**	https://discuss.elastic.co/t/kibana-8-15-1-security-update-esa-2024-27-esa-2024-28/366119	A-ELA-KIBA-180924/127
Vendor: erjemin					
Product: roll_cms					
Affected Version(s): * Up to (excluding) 2024-08-31					
Generation of Error Message Containing Sensitive	08-Sep-2024	5.3	A vulnerability was found in erjemin roll_cms up to 1484fe2c4e0805946a7bcf46218509fc	N/A	A-ERJ-ROLL-180924/128

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
Information			b34883a9. It has been classified as problematic. This affects an unknown part of the file roll_cms/roll_cms/views.py. The manipulation leads to information exposure through error message. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. **CVE ID: CVE-2024-8571**		
Vendor: ethyca					
Product: fides					
Affected Version(s): * Up to (excluding) 2.44.0					
Observable Discrepancy	04-Sep-2024	5.3	Fides is an open-source privacy engineering platform. Prior to version 2.44.0, a timing-based username enumeration vulnerability exists in Fides Webserver authentication. This vulnerability allows an unauthenticated attacker to determine the existence of valid	https://github.com/ethyca/fides/commit/457b0e9df9f0d337133d6078bca6ed88bbc745f4, https://github.com/ethyca/fides/security/advisories/GHSA-2h46-8gf5-fmxv	A-ETH-FIDE-180924/129

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
			usernames by analyzing the time it takes for the server to respond to login requests. The discrepancy in response times between valid and invalid usernames can be leveraged to enumerate users on the system. This vulnerability enables a timing-based username enumeration attack. An attacker can systematically guess and verify which usernames are valid by measuring the server's response time to authentication requests. This information can be used to conduct further attacks on authentication such as password brute-forcing and credential stuffing. The vulnerability has been patched in Fides version `2.44.0`. Users are advised to upgrade to this version or later to secure their systems against this threat. There are no workarounds.		

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
			CVE ID: CVE-2024-45052		
Affected Version(s): From (including) 2.19.0 Up to (excluding) 2.44.0					
Improper Control of Generation of Code ('Code Injection')	04-Sep-2024	7.2	Fides is an open-source privacy engineering platform. Starting in version 2.19.0 and prior to version 2.44.0, the Email Templating feature uses Jinja2 without proper input sanitization or rendering environment restrictions, allowing for Server-Side Template Injection that grants Remote Code Execution to privileged users. A privileged user refers to an Admin UI user with the default `Owner` or `Contributor` role, who can escalate their access and execute code on the underlying Fides Webserver container where the Jinja template rendering function is executed. The vulnerability has been patched in Fides version `2.44.0`. Users are advised to upgrade to this version or	https://github.com/ethyca/fides/commit/829cbd9cb5ef9c814fbac1ed6800e8d939d359c5, https://github.com/ethyca/fides/security/advisories/GHSA-c34r-238x-f7qx	A-ETH-FIDE-180924/130

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
			later to secure their systems against this threat. There are no workarounds. **CVE ID: CVE-2024-45053**		
Vendor: fabianros					
Product: hospital_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-2024	9.8	A vulnerability was found in code-projects Hospital Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file index.php of the component Login. The manipulation of the argument username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8368**	N/A	A-FAB-HOSP-180924/131
Improper Neutralization of Special Elements used in an SQL Command	08-Sep-2024	9.8	A vulnerability has been found in code-projects Hospital Management System 1.0 and classified as critical. Affected by this vulnerability is an	N/A	A-FAB-HOSP-180924/132

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
('SQL Injection')			unknown functionality of the file user-login.php. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8569**		
Vendor: forcepoint					
Product: email_security					
Affected Version(s): * Up to (excluding) 8.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Sep-2024	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Forcepoint Email Security (Real Time Monitor modules) allows Reflected XSS.This issue affects Email Security: before 8.5.5 HF003. **CVE ID: CVE-2024-2166**	https://support.forcepoint.com/s/article/000042397	A-FOR-EMAI-180924/133
Affected Version(s): 8.5.5					
Improper Neutralization of Input During Web Page	04-Sep-2024	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site	https://support.forcepoint.com/s/article/000042397	A-FOR-EMAI-180924/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Scripting') vulnerability in Forcepoint Email Security (Real Time Monitor modules) allows Reflected XSS.This issue affects Email Security: before 8.5.5 HF003. **CVE ID: CVE-2024-2166**		
Vendor: Github					
Product: actions\/artifact					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.1.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Sep-2024	7.5	actions/artifact is the GitHub ToolKit for developing GitHub Actions. Versions of `actions/artifact` before 2.1.7 are vulnerable to arbitrary file write when using `downloadArtifactInternal`, `downloadArtifactPublic`, or `streamExtractExternal` for extracting a specifically crafted artifact that contains path traversal filenames. Users are advised to upgrade to version 2.1.7 or higher. There are no known workarounds for this issue.	https://github.com/actions/toolkit/pull/1724, https://github.com/actions/toolkit/security/advisories/GHSA-6q32-hq47-5qq3	A-GIT-ACTI-180924/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42471		
Product: actions_toolkit					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Sep-2024	7.5	actions/artifact is the GitHub ToolKit for developing GitHub Actions. Versions of `actions/artifact` before 2.1.7 are vulnerable to arbitrary file write when using `downloadArtifactInternal`, `downloadArtifactPublic`, or `streamExtractExternal` for extracting a specifically crafted artifact that contains path traversal filenames. Users are advised to upgrade to version 2.1.7 or higher. There are no known workarounds for this issue. **CVE ID: CVE-2024-42471**	https://github.com/actions/toolkit/pull/1724, https://github.com/actions/toolkit/security/advisories/GHSA-6q32-hq47-5qq3	A-GIT-ACTI-180924/136
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): From (including) 11.2.0 Up to (excluding) 17.1.7					
N/A	12-Sep-2024	7.5	An issue has been discovered in GitLab EE affecting all versions starting from 11.2 before	N/A	A-GIT-GITL-180924/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			17.1.7, all versions starting from 17.2 before 17.2.5, all versions starting from 17.3 before 17.3.2. It was possible for a guest to read the source code of a private project by using group templates. **CVE ID: CVE-2024-4660**		
Affected Version(s): From (including) 12.9.0 Up to (excluding) 17.1.7					
URL Redirection to Untrusted Site ('Open Redirect')	12-Sep-2024	6.1	An issue has been discovered in GitLab EE affecting all versions starting from 12.9 before 17.1.7, 17.2 before 17.2.5, and 17.3 before 17.3.2. Under certain conditions an open redirect vulnerability could allow for an account takeover by breaking the OAuth flow. **CVE ID: CVE-2024-4612**	N/A	A-GIT-GITL-180924/138
Affected Version(s): From (including) 13.3.0 Up to (excluding) 17.1.7					
Incorrect Authorization	12-Sep-2024	9.1	An issue was discovered in GitLab-EE starting with version 13.3 before 17.1.7, 17.2 before 17.2.5, and 17.3 before 17.3.2 that would allow an attacker to modify	N/A	A-GIT-GITL-180924/139

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
			an on-demand DAST scan without permissions and leak variables. **CVE ID: CVE-2024-2743**		
Affected Version(s): From (including) 15.10.0 Up to (excluding) 17.1.7					
Generation of Error Message Containing Sensitive Information	12-Sep-2024	6.5	An issue has been discovered discovered in GitLab EE/CE affecting all versions starting from 15.10 before 17.1.7, all versions starting from 17.2 before 17.2.5, all versions starting from 17.3 before 17.3.2 will disclose user password from repository mirror configuration. **CVE ID: CVE-2024-5435**	N/A	A-GIT-GITL-180924/140
Affected Version(s): From (including) 16.11.0 Up to (excluding) 17.1.7					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Sep-2024	8.8	An issue has been discovered in GitLab EE affecting all versions starting from 16.11 prior to 17.1.7, from 17.2 prior to 17.2.5, and from 17.3 prior to 17.3.2. Due to incomplete input filtering, it was possible to inject commands into a connected Cube server.	N/A	A-GIT-GITL-180924/141

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
			CVE ID: CVE-2024-8640		
Affected Version(s): From (including) 16.4.0 Up to (excluding) 17.1.7					
N/A	12-Sep-2024	7.5	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.4 prior to 17.1.7, starting from 17.2 prior to 17.2.5, starting from 17.3 prior to 17.3.2 which could cause Denial of Service via sending a large `glm_source` parameter. **CVE ID: CVE-2024-8124**	N/A	A-GIT-GITL-180924/142
Affected Version(s): From (including) 16.6.0 Up to (excluding) 17.1.7					
N/A	12-Sep-2024	7.2	A privilege escalation issue has been discovered in GitLab EE affecting all versions starting from 16.6 prior to 17.1.7, from 17.2 prior to 17.2.5, and from 17.3 prior to 17.3.2. A user assigned the Admin Group Member custom role could have escalated their privileges to include other custom roles. **CVE ID: CVE-2024-8631**	N/A	A-GIT-GITL-180924/143
Affected Version(s): From (including) 16.8.0 Up to (excluding) 17.1.7					

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
Server-Side Request Forgery (SSRF)	12-Sep-2024	6.5	A server-side request forgery issue has been discovered in GitLab EE affecting all versions starting from 16.8 prior to 17.1.7, from 17.2 prior to 17.2.5, and from 17.3 prior to 17.3.2. It was possible for an attacker to make requests to internal resources using a custom Maven Dependency Proxy URL **CVE ID: CVE-2024-8635**	N/A	A-GIT-GITL-180924/144
Affected Version(s): From (including) 16.9.7 Up to (excluding) 17.1.7					
N/A	12-Sep-2024	8.1	An issue has been discovered in GitLab EE/CE affecting all versions from 16.9.7 prior to 17.1.7, 17.2 prior to 17.2.5, and 17.3 prior to 17.3.2. An improper input validation error allows attacker to squat on accounts via linking arbitrary unclaimed provider identities when JWT authentication is configured. **CVE ID: CVE-2024-8754**	N/A	A-GIT-GITL-180924/145

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.7					
N/A	12-Sep-2024	4.3	An issue was discovered in GitLab-CE/EE affecting all versions starting with 17.0 before 17.1.7, 17.2 before 17.2.5, and 17.3 before 17.3.2. An attacker as a guest user was able to access commit information via the release Atom endpoint, contrary to permissions. **CVE ID: CVE-2024-6389**	N/A	A-GIT-GITL-180924/146
Affected Version(s): From (including) 17.1.0 Up to (excluding) 17.1.7					
N/A	12-Sep-2024	3.5	An issue has been discovered in GitLab affecting all versions starting from 17.1 to 17.1.7, 17.2 prior to 17.2.5 and 17.3 prior to 17.3.2. A crafted URL could be used to trick a victim to trust an attacker controlled application. **CVE ID: CVE-2024-6446**	N/A	A-GIT-GITL-180924/147
Affected Version(s): From (including) 17.2.0 Up to (excluding) 17.2.5					
Incorrect Authorization	12-Sep-2024	9.1	An issue was discovered in GitLab-EE starting with version 13.3 before 17.1.7, 17.2 before 17.2.5, and	N/A	A-GIT-GITL-180924/148

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
			17.3 before 17.3.2 that would allow an attacker to modify an on-demand DAST scan without permissions and leak variables. **CVE ID: CVE-2024-2743**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Sep-2024	8.8	An issue has been discovered in GitLab EE affecting all versions starting from 16.11 prior to 17.1.7, from 17.2 prior to 17.2.5, and from 17.3 prior to 17.3.2. Due to incomplete input filtering, it was possible to inject commands into a connected Cube server. **CVE ID: CVE-2024-8640**	N/A	A-GIT-GITL-180924/149
N/A	12-Sep-2024	8.1	An issue has been discovered in GitLab EE/CE affecting all versions from 16.9.7 prior to 17.1.7, 17.2 prior to 17.2.5, and 17.3 prior to 17.3.2. An improper input validation error allows attacker to squat on accounts via linking arbitrary unclaimed provider identities when	N/A	A-GIT-GITL-180924/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JWT authentication is configured. **CVE ID: CVE-2024-8754**		
N/A	12-Sep-2024	7.5	An issue has been discovered in GitLab EE affecting all versions starting from 11.2 before 17.1.7, all versions starting from 17.2 before 17.2.5, all versions starting from 17.3 before 17.3.2. It was possible for a guest to read the source code of a private project by using group templates. **CVE ID: CVE-2024-4660**	N/A	A-GIT-GITL-180924/151
N/A	12-Sep-2024	7.5	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.4 prior to 17.1.7, starting from 17.2 prior to 17.2.5, starting from 17.3 prior to 17.3.2 which could cause Denial of Service via sending a large `glm_source` parameter. **CVE ID: CVE-2024-8124**	N/A	A-GIT-GITL-180924/152
N/A	12-Sep-2024	7.2	A privilege escalation issue has been discovered in	N/A	A-GIT-GITL-180924/153

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
			GitLab EE affecting all versions starting from 16.6 prior to 17.1.7, from 17.2 prior to 17.2.5, and from 17.3 prior to 17.3.2. A user assigned the Admin Group Member custom role could have escalated their privileges to include other custom roles. **CVE ID: CVE-2024-8631**		
Generation of Error Message Containing Sensitive Information	12-Sep-2024	6.5	An issue has been discovered discovered in GitLab EE/CE affecting all versions starting from 15.10 before 17.1.7, all versions starting from 17.2 before 17.2.5, all versions starting from 17.3 before 17.3.2 will disclose user password from repository mirror configuration. **CVE ID: CVE-2024-5435**	N/A	A-GIT-GITL-180924/154
Server-Side Request Forgery (SSRF)	12-Sep-2024	6.5	A server-side request forgery issue has been discovered in GitLab EE affecting all versions starting from 16.8 prior to 17.1.7, from 17.2	N/A	A-GIT-GITL-180924/155

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
			prior to 17.2.5, and from 17.3 prior to 17.3.2. It was possible for an attacker to make requests to internal resources using a custom Maven Dependency Proxy URL **CVE ID: CVE-2024-8635**		
URL Redirection to Untrusted Site ('Open Redirect')	12-Sep-2024	6.1	An issue has been discovered in GitLab EE affecting all versions starting from 12.9 before 17.1.7, 17.2 before 17.2.5, and 17.3 before 17.3.2. Under certain conditions an open redirect vulnerability could allow for an account takeover by breaking the OAuth flow. **CVE ID: CVE-2024-4612**	N/A	A-GIT-GITL-180924/156
N/A	12-Sep-2024	4.3	An issue was discovered in GitLab-CE/EE affecting all versions starting with 17.0 before 17.1.7, 17.2 before 17.2.5, and 17.3 before 17.3.2. An attacker as a guest user was able to access commit information via the	N/A	A-GIT-GITL-180924/157

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
			release Atom endpoint, contrary to permissions. **CVE ID: CVE-2024-6389**		
N/A	12-Sep-2024	3.5	An issue has been discovered in GitLab affecting all versions starting from 17.1 to 17.1.7, 17.2 prior to 17.2.5 and 17.3 prior to 17.3.2. A crafted URL could be used to trick a victim to trust an attacker controlled application. **CVE ID: CVE-2024-6446**	N/A	A-GIT-GITL-180924/158
Affected Version(s): From (including) 17.3.0 Up to (excluding) 17.3.2					
Incorrect Authorization	12-Sep-2024	9.1	An issue was discovered in GitLab-EE starting with version 13.3 before 17.1.7, 17.2 before 17.2.5, and 17.3 before 17.3.2 that would allow an attacker to modify an on-demand DAST scan without permissions and leak variables. **CVE ID: CVE-2024-2743**	N/A	A-GIT-GITL-180924/159
Improper Neutralization of Special Elements used in a	12-Sep-2024	8.8	An issue has been discovered in GitLab EE affecting all versions starting from 16.11 prior to 17.1.7, from 17.2	N/A	A-GIT-GITL-180924/160

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
Command ('Command Injection')			prior to 17.2.5, and from 17.3 prior to 17.3.2. Due to incomplete input filtering, it was possible to inject commands into a connected Cube server. **CVE ID: CVE-2024-8640**		
N/A	12-Sep-2024	8.1	An issue has been discovered in GitLab EE/CE affecting all versions from 16.9.7 prior to 17.1.7, 17.2 prior to 17.2.5, and 17.3 prior to 17.3.2. An improper input validation error allows attacker to squat on accounts via linking arbitrary unclaimed provider identities when JWT authentication is configured. **CVE ID: CVE-2024-8754**	N/A	A-GIT-GITL-180924/161
N/A	12-Sep-2024	7.5	An issue has been discovered in GitLab EE affecting all versions starting from 11.2 before 17.1.7, all versions starting from 17.2 before 17.2.5, all versions starting from 17.3 before 17.3.2. It was	N/A	A-GIT-GITL-180924/162

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
			possible for a guest to read the source code of a private project by using group templates. **CVE ID: CVE-2024-4660**		
N/A	12-Sep-2024	7.5	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.4 prior to 17.1.7, starting from 17.2 prior to 17.2.5, starting from 17.3 prior to 17.3.2 which could cause Denial of Service via sending a large `glm_source` parameter. **CVE ID: CVE-2024-8124**	N/A	A-GIT-GITL-180924/163
N/A	12-Sep-2024	7.2	A privilege escalation issue has been discovered in GitLab EE affecting all versions starting from 16.6 prior to 17.1.7, from 17.2 prior to 17.2.5, and from 17.3 prior to 17.3.2. A user assigned the Admin Group Member custom role could have escalated their privileges to include other custom roles.	N/A	A-GIT-GITL-180924/164

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
			CVE ID: CVE-2024-8631		
Generation of Error Message Containing Sensitive Information	12-Sep-2024	6.5	An issue has been discovered discovered in GitLab EE/CE affecting all versions starting from 15.10 before 17.1.7, all versions starting from 17.2 before 17.2.5, all versions starting from 17.3 before 17.3.2 will disclose user password from repository mirror configuration. **CVE ID: CVE-2024-5435**	N/A	A-GIT-GITL-180924/165
Server-Side Request Forgery (SSRF)	12-Sep-2024	6.5	A server-side request forgery issue has been discovered in GitLab EE affecting all versions starting from 16.8 prior to 17.1.7, from 17.2 prior to 17.2.5, and from 17.3 prior to 17.3.2. It was possible for an attacker to make requests to internal resources using a custom Maven Dependency Proxy URL **CVE ID: CVE-2024-8635**	N/A	A-GIT-GITL-180924/166

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
URL Redirection to Untrusted Site ('Open Redirect')	12-Sep-2024	6.1	An issue has been discovered in GitLab EE affecting all versions starting from 12.9 before 17.1.7, 17.2 before 17.2.5, and 17.3 before 17.3.2. Under certain conditions an open redirect vulnerability could allow for an account takeover by breaking the OAuth flow. **CVE ID: CVE-2024-4612**	N/A	A-GIT-GITL-180924/167
N/A	12-Sep-2024	4.3	An issue was discovered in GitLab-CE/EE affecting all versions starting with 17.0 before 17.1.7, 17.2 before 17.2.5, and 17.3 before 17.3.2. An attacker as a guest user was able to access commit information via the release Atom endpoint, contrary to permissions. **CVE ID: CVE-2024-6389**	N/A	A-GIT-GITL-180924/168
N/A	12-Sep-2024	3.5	An issue has been discovered in GitLab affecting all versions starting from 17.1 to 17.1.7, 17.2 prior to 17.2.5 and 17.3 prior to	N/A	A-GIT-GITL-180924/169

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
			17.3.2. A crafted URL could be used to trick a victim to trust an attacker controlled application. **CVE ID: CVE-2024-6446**		
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 128.0.6613.137					
Out-of-bounds Write	11-Sep-2024	8.8	Heap buffer overflow in Skia in Google Chrome prior to 128.0.6613.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-8636**	N/A	A-GOO-CHRO-180924/170
Use After Free	11-Sep-2024	8.8	Use after free in Media Router in Google Chrome on Android prior to 128.0.6613.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-8637**	N/A	A-GOO-CHRO-180924/171

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	11-Sep-2024	8.8	Type Confusion in V8 in Google Chrome prior to 128.0.6613.137 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-8638**	N/A	A-GOO-CHRO-180924/172
Use After Free	11-Sep-2024	8.8	Use after free in Autofill in Google Chrome on Android prior to 128.0.6613.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-8639**	N/A	A-GOO-CHRO-180924/173
Vendor: gouniverse					
Product: golang_cms					
Affected Version(s): * Up to (excluding) 1.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Sep-2024	6.1	A vulnerability was found in Gouniverse GoLang CMS 1.4.0. It has been declared as problematic. This vulnerability affects the function PageRenderHtmlByAlias of the file	https://github.com/gouniverse/cms/commit/3e661cdfb4beeb9fe2ad507cdb8104c0b17d072c	A-GOU-GOLA-180924/174

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
			FrontendHandler.go. The manipulation of the argument alias leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 1.4.1 is able to address this issue. The patch is identified as 3e661cdfb4beeb9fe2ad507cdb8104c0b17d072c. It is recommended to upgrade the affected component. **CVE ID: CVE-2024-8572**		
Vendor: halo					
Product: halo					
Affected Version(s): * Up to (excluding) 2.17.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-2024	6.1	Halo is an open source website building tool. A security vulnerability has been identified in versions prior to 2.17.0 of the Halo project. This vulnerability allows an attacker to execute malicious scripts in the user's browser through specific HTML and JavaScript code,	https://github.com/halo-dev/halo/security/advisories/GHSA-x3rj-3x75-vw4g	A-HAL-HALO-180924/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to a Cross-Site Scripting (XSS) attack. Users are advised to upgrade to version 2.17.0+. There are no known workarounds for this vulnerability. **CVE ID: CVE-2024-43792**		
Affected Version(s): * Up to (excluding) 2.19.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-2024	6.4	Halo is an open source website building tool. A security vulnerability has been identified in versions prior to 2.19.0 of the Halo project. This vulnerability allows an attacker to execute malicious scripts in the user's browser through specific HTML and JavaScript code, potentially leading to a Cross-Site Scripting (XSS) attack. This vulnerability is fixed in 2.19.0. **CVE ID: CVE-2024-43793**	N/A	A-HAL-HALO-180924/176
Vendor: Haproxy					
Product: haproxy					
Affected Version(s): 3.1					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Sep-2024	7.5	HAProxy 2.9.x before 2.9.10, 3.0.x before 3.0.4, and 3.1.x through 3.1-dev6 allows a remote denial of service. **CVE ID: CVE-2024-45506**	N/A	A-HAP-HAPR-180924/177
Affected Version(s): From (including) 2.9.0 Up to (excluding) 2.9.10					
N/A	04-Sep-2024	7.5	HAProxy 2.9.x before 2.9.10, 3.0.x before 3.0.4, and 3.1.x through 3.1-dev6 allows a remote denial of service. **CVE ID: CVE-2024-45506**	N/A	A-HAP-HAPR-180924/178
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.4					
N/A	04-Sep-2024	7.5	HAProxy 2.9.x before 2.9.10, 3.0.x before 3.0.4, and 3.1.x through 3.1-dev6 allows a remote denial of service. **CVE ID: CVE-2024-45506**	N/A	A-HAP-HAPR-180924/179
Vendor: hashicorp					
Product: vault					
Affected Version(s): * Up to (excluding) 1.16.9					
Insertion of Sensitive Information into Log File	02-Sep-2024	6.5	Vault Community Edition and Vault Enterprise experienced a regression where functionality that HMAC'd sensitive headers in the	https://discuss.hashicorp.com/t/hcsec-2024-18-vault-leaks-client-token-and-token-accessor-in-audit-devices/	A-HAS-VAUL-180924/180

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
			configured audit device, specifically client tokens and token accessors, was removed. This resulted in the plaintext values of client tokens and token accessors being stored in the audit log. This vulnerability, CVE-2024-8365, was fixed in Vault Community Edition and Vault Enterprise 1.17.5 and Vault Enterprise 1.16.9. **CVE ID: CVE-2024-8365**		
Affected Version(s): * Up to (excluding) 1.17.5					
Insertion of Sensitive Information into Log File	02-Sep-2024	6.5	Vault Community Edition and Vault Enterprise experienced a regression where functionality that HMAC'd sensitive headers in the configured audit device, specifically client tokens and token accessors, was removed. This resulted in the plaintext values of client tokens and token accessors being stored in the audit log. This vulnerability, CVE-2024-8365, was	https://discuss.hashicorp.com/t/hcsec-2024-18-vault-leaks-client-token-and-token-accessor-in-audit-devices/	A-HAS-VAUL-180924/181

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
			fixed in Vault Community Edition and Vault Enterprise 1.17.5 and Vault Enterprise 1.16.9. **CVE ID: CVE-2024-8365**		
Affected Version(s): From (including) 1.17.0 Up to (excluding) 1.17.5					
Insertion of Sensitive Information into Log File	02-Sep-2024	6.5	Vault Community Edition and Vault Enterprise experienced a regression where functionality that HMAC'd sensitive headers in the configured audit device, specifically client tokens and token accessors, was removed. This resulted in the plaintext values of client tokens and token accessors being stored in the audit log. This vulnerability, CVE-2024-8365, was fixed in Vault Community Edition and Vault Enterprise 1.17.5 and Vault Enterprise 1.16.9. **CVE ID: CVE-2024-8365**	https://discuss.hashicorp.com/t/hcsec-2024-18-vault-leaks-client-token-and-token-accessor-in-audit-devices/	A-HAS-VAUL-180924/182
Vendor: helloasso					
Product: helloasso					
Affected Version(s): * Up to (excluding) 1.1.11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	05-Sep-2024	4.3	The HelloAsso plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ha_ajax' function in all versions up to, and including, 1.1.10. This makes it possible for authenticated attackers, with Contributor-level access and above, to update plugin options, potentially disrupting the service. **CVE ID: CVE-2024-7605**	https://plugins.trac.wordpress.org/changeset/3145151/	A-HEL-HELL-180924/183
Vendor: htmldoc_project					
Product: htmldoc					
Affected Version(s): * Up to (excluding) 1.9.19					
Out-of-bounds Write	01-Sep-2024	9.8	HTMLDOC before 1.9.19 has an out-of-bounds write in parse_paragraph in ps-pdf.cxx because of an attempt to strip leading whitespace from a whitespace-only node. **CVE ID: CVE-2024-45508**	https://github.com/michaelrsweet/htmldoc/commit/2d5b2ab9ddbf2aee2209010cebc11efdd1cab6e2, https://github.com/michaelrsweet/htmldoc/issues/528	A-HTM-HTML-180924/184
Vendor: IBM					
Product: aspera_faspex					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.0.10					
N/A	05-Sep-2024	8.1	IBM Aspera Faspex 5.0.0 through 5.0.9 could allow a user to bypass intended access restrictions and conduct resource modification. **CVE ID: CVE-2024-45098**	https://www.ibm.com/support/pages/node/7167255	A-IBM-ASPE-180924/185
Interpretation Conflict	05-Sep-2024	7.1	IBM Aspera Faspex 5.0.0 through 5.0.9 could allow a user to bypass intended access restrictions and conduct resource modification. **CVE ID: CVE-2024-45097**	https://www.ibm.com/support/pages/node/7167255	A-IBM-ASPE-180924/186
N/A	05-Sep-2024	6.5	IBM Aspera Faspex 5.0.0 through 5.0.9 could allow a user with access to the package to obtain sensitive information through a directory listing. **CVE ID: CVE-2024-45096**	https://www.ibm.com/support/pages/node/7167255	A-IBM-ASPE-180924/187
Product: maximo_application_suite					
Affected Version(s): 8.10					
Use of a Broken or Risky Cryptographic Algorithm	07-Sep-2024	7.5	IBM Maximo Application Suite - Manage Component 8.10, 8.11, and 9.0 uses weaker than expected	https://exchange.xforce.ibmcloud.com/vulnerabilities/292799, https://www.ibm.com/support	A-IBM-MAXI-180924/188

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
			cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. **CVE ID: CVE-2024-37068**	/pages/node/7167725	
Affected Version(s): 8.11					
Use of a Broken or Risky Cryptographic Algorithm	07-Sep-2024	7.5	IBM Maximo Application Suite - Manage Component 8.10, 8.11, and 9.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. **CVE ID: CVE-2024-37068**	https://exchange.xforce.ibmcloud.com/vulnerabilities/292799, https://www.ibm.com/support/pages/node/7167725	A-IBM-MAXI-180924/189
Affected Version(s): 9.0					
Use of a Broken or Risky Cryptographic Algorithm	07-Sep-2024	7.5	IBM Maximo Application Suite - Manage Component 8.10, 8.11, and 9.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. **CVE ID: CVE-2024-37068**	https://exchange.xforce.ibmcloud.com/vulnerabilities/292799, https://www.ibm.com/support/pages/node/7167725	A-IBM-MAXI-180924/190
Product: mq_operator					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.0.26					
Allocation of Resources Without Limits or Throttling	07-Sep-2024	5.5	IBM MQ Operator 2.0.26 and 3.2.4 could allow a local user to cause a denial of service due to improper memory allocation causing a segmentation fault. **CVE ID: CVE-2024-40680**	https://exchange.xforce.ibmcloud.com/vulnerabilities/297611, https://www.ibm.com/support/pages/node/7167732	A-IBM-MQ_O-180924/191
Affected Version(s): 3.2.4					
Allocation of Resources Without Limits or Throttling	07-Sep-2024	5.5	IBM MQ Operator 2.0.26 and 3.2.4 could allow a local user to cause a denial of service due to improper memory allocation causing a segmentation fault. **CVE ID: CVE-2024-40680**	https://exchange.xforce.ibmcloud.com/vulnerabilities/297611, https://www.ibm.com/support/pages/node/7167732	A-IBM-MQ_O-180924/192
Product: openpages_grc_platform					
Affected Version(s): From (including) 8.3 Up to (excluding) 8.3.0.2					
N/A	10-Sep-2024	4.3	IBM OpenPages 8.3 and 9.0 potentially exposes information about client-side source code through use of JavaScript source maps to unauthorized users. **CVE ID: CVE-2024-27257**	https://exchange.xforce.ibmcloud.com/vulnerabilities/283966, https://www.ibm.com/support/pages/node/7167702	A-IBM-OPEN-180924/193
Product: openpages_with_watson					
Affected Version(s): From (including) 9.0 Up to (excluding) 9.0.0.3					

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
N/A	10-Sep-2024	4.3	IBM OpenPages 8.3 and 9.0 potentially exposes information about client-side source code through use of JavaScript source maps to unauthorized users. **CVE ID: CVE-2024-27257**	https://exchange.xforce.ibmcloud.com/vulnerabilities/283966, https://www.ibm.com/support/pages/node/7167702	A-IBM-OPEN-180924/194
Product: webmethods_integration					
Affected Version(s): 10.15					
Unrestricted Upload of File with Dangerous Type	04-Sep-2024	9.9	IBM webMethods Integration 10.15 could allow an authenticated user to upload and execute arbitrary files which could be executed on the underlying operating system. **CVE ID: CVE-2024-45076**	https://www.ibm.com/support/pages/node/7167245	A-IBM-WEBM-180924/195
N/A	04-Sep-2024	8.8	IBM webMethods Integration 10.15 could allow an authenticated user to create scheduler tasks that would allow them to escalate their privileges to administrator due to missing authentication. **CVE ID: CVE-2024-45075**	https://www.ibm.com/support/pages/node/7167245	A-IBM-WEBM-180924/196

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 Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Sep-2024	6.5	IBM webMethods Integration 10.15 could allow an authenticated user to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. **CVE ID: CVE-2024-45074**	https://www.ibm.com/support/pages/node/7167245	A-IBM-WEBM-180924/197
Vendor: idec					
Product: windldr					
Affected Version(s): * Up to (excluding) 9.2.0					
Cleartext Storage of Sensitive Information	04-Sep-2024	8.1	Cleartext storage of sensitive information vulnerability exists in WindLDR and WindO/I-NV4. If this vulnerability is exploited, an attacker who obtained the product's project file may obtain user credentials of the PLC or Operator Interfaces. As a result, an attacker may be able to manipulate and/or suspend the PLC and Operator Interfaces by	https://us.idec.com/media/24-RD-0219-EN.pdf	A-IDE-WIND-180924/198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accessing or hijacking them. **CVE ID: CVE-2024-41716**		
Product: windo\/i-nv4					
Affected Version(s): * Up to (excluding) 3.1.0					
Cleartext Storage of Sensitive Informatio n	04-Sep-2024	8.1	Cleartext storage of sensitive information vulnerability exists in WindLDR and WindO/I-NV4. If this vulnerability is exploited, an attacker who obtained the product's project file may obtain user credentials of the PLC or Operator Interfaces. As a result, an attacker may be able to manipulate and/or suspend the PLC and Operator Interfaces by accessing or hijacking them. **CVE ID: CVE-2024-41716**	https://us.idec.com/media/24-RD-0219-EN.pdf	A-IDE-WIND-180924/199
Vendor: identityautomation					
Product: rapididentity					
Affected Version(s): * Up to (including) 2023.0.2					
Improper Restriction of Excessive Authentica	05-Sep-2024	5.9	RapidIdentity LTS through 2023.0.2 and Cloud through 2024.08.0 improperly restricts excessive authentication	N/A	A-IDE-RAPI-180924/200

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
tion Attempts			attempts and allows a remote attacker to cause a denial of service via the username parameters. **CVE ID: CVE-2024-45589**		
Affected Version(s): * Up to (including) 2024.08.0					
Improper Restriction of Excessive Authentication Attempts	05-Sep-2024	5.9	RapidIdentity LTS through 2023.0.2 and Cloud through 2024.08.0 improperly restricts excessive authentication attempts and allows a remote attacker to cause a denial of service via the username parameters. **CVE ID: CVE-2024-45589**	N/A	A-IDE-RAPI-180924/201
Vendor: incsub					
Product: forminator					
Affected Version(s): * Up to (excluding) 1.34.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Sep-2024	6.1	Cross-site scripting vulnerability exists in Forminator versions prior to 1.34.1. If this vulnerability is exploited, an arbitrary script may be executed on the web browser of the user who follows a crafted URL and accesses the webpage with	https://plugins.trac.wordpress.org/changeset?new=3135507%40forminator%2Ftrunk%2Fassets%2Fjs%2Ffront%2Ffront.mergetags.js&old=3111152%40forminator%2Ftrunk%2Fassets%2Fjs%2Ffront	A-INC-FORM-180924/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web form created by Forminator. **CVE ID: CVE-2024-45625**	%2Ffront.mergetags.js	
Vendor: infinitumform					
Product: geo_controller					
Affected Version(s): * Up to (including) 8.6.9					
Missing Authorization	05-Sep-2024	5.3	The Geo Controller plugin for WordPress is vulnerable to unauthorized shortcode execution due to missing authorization and capability checks on the ajax_shortcode_cache function in all versions up to, and including, 8.6.9. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes available on the target site. **CVE ID: CVE-2024-7381**	N/A	A-INF-GEO_-180924/203
Missing Authorization	05-Sep-2024	4.3	The Geo Controller plugin for WordPress is vulnerable to unauthorized menu creation/deletion due to missing capability checks on the	N/A	A-INF-GEO_-180924/204

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
			ajax__geolocate_menu and ajax__geolocate_remove_menu functions in all versions up to, and including, 8.6.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create or delete WordPress menus. **CVE ID: CVE-2024-7380**		
Vendor: istyle					
Product: \@cosme					
Affected Version(s): * Up to (excluding) 5.69.0					
N/A	09-Sep-2024	4.3	Improper authorization in handler for custom URL scheme issue in "@cosme" App for Android versions prior 5.69.0 and "@cosme" App for iOS versions prior to 6.74.0 allows an attacker to lead a user to access an arbitrary website via the vulnerable App. As a result, the user may become a victim of a phishing attack. **CVE ID: CVE-2024-45203**	N/A	A-IST-\@CO-180924/205

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 6.74.0					
N/A	09-Sep-2024	4.3	Improper authorization in handler for custom URL scheme issue in "@cosme" App for Android versions prior 5.69.0 and "@cosme" App for iOS versions prior to 6.74.0 allows an attacker to lead a user to access an arbitrary website via the vulnerable App. As a result, the user may become a victim of a phishing attack. **CVE ID: CVE-2024-45203**	N/A	A-IST-\@CO-180924/206
Vendor: ivanti					
Product: cloud_services_appliance					
Affected Version(s): 4.6					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Sep-2024	7.2	An OS command injection vulnerability in Ivanti Cloud Services Appliance versions 4.6 Patch 518 and before allows a remote authenticated attacker to obtain remote code execution. The attacker must have admin level privileges to exploit this vulnerability.	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Service-Appliance-CSA-CVE-2024-8190	A-IVA-CLOU-180924/207

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
			CVE ID: CVE-2024-8190		
Product: endpoint_manager					
Affected Version(s): * Up to (excluding) 2022					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Sep-2024	9.8	SQL injection in the management console of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to achieve remote code execution. **CVE ID: CVE-2024-8191**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/208
Deserialization of Untrusted Data	12-Sep-2024	9.8	Deserialization of untrusted data in the agent portal of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to achieve remote code execution. **CVE ID: CVE-2024-29847**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/209
N/A	10-Sep-2024	8.8	Weak authentication in Patch Management of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker to access	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/210

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
			restricted functionality. **CVE ID: CVE-2024-8322**		
Missing Authentication for Critical Function	10-Sep-2024	8.6	Missing authentication in Network Isolation of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to isolate managed devices from the network. **CVE ID: CVE-2024-8321**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/211
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-32840**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/212
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/213

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
			CVE ID: CVE-2024-32842		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-32843**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/214
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-32845**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/215
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-32846**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/216

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 Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-32848**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/217
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-34779**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/218
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-34783**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/219
Improper Neutralization of	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022	https://forums.ivanti.com/s/article/Security-	A-IVA-ENDP-180924/220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-34785**	Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	
Uncontrolled Search Path Element	10-Sep-2024	6.7	An uncontrolled search path in the agent of Ivanti EPM before 2022 SU6, or the 2024 September update allows a local authenticated attacker with admin privileges to escalate their privileges to SYSTEM. **CVE ID: CVE-2024-8441**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/221
Missing Authentication for Critical Function	10-Sep-2024	5.3	Missing authentication in Network Isolation of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to spoof Network Isolation status of managed devices. **CVE ID: CVE-2024-8320**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/222
Affected Version(s): 2022					

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 Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Sep-2024	9.8	SQL injection in the management console of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to achieve remote code execution. **CVE ID: CVE-2024-8191**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/223
Deserialization of Untrusted Data	12-Sep-2024	9.8	Deserialization of untrusted data in the agent portal of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to achieve remote code execution. **CVE ID: CVE-2024-29847**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/224
N/A	10-Sep-2024	8.8	Weak authentication in Patch Management of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker to access restricted functionality. **CVE ID: CVE-2024-8322**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/225

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
Missing Authentication for Critical Function	10-Sep-2024	8.6	Missing authentication in Network Isolation of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to isolate managed devices from the network. **CVE ID: CVE-2024-8321**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/226
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-32840**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/227
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-32842**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/228
Improper Neutralizat	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti	https://forums.ivanti.com/s/art	A-IVA-ENDP-180924/229

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
ion of Special Elements used in an SQL Command ('SQL Injection')			EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-32843**	icle/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-32845**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/230
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-32846**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/231
Improper Neutralization of Special Elements	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-	A-IVA-ENDP-180924/232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-32848**	2024-for-EPM-2024-and-EPM-2022	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-34779**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/233
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-34783**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/234
Improper Neutralization of Special Elements used in an SQL Command	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/235

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
('SQL Injection')			admin privileges to achieve remote code execution. **CVE ID: CVE-2024-34785**		
Uncontrolled Search Path Element	10-Sep-2024	6.7	An uncontrolled search path in the agent of Ivanti EPM before 2022 SU6, or the 2024 September update allows a local authenticated attacker with admin privileges to escalate their privileges to SYSTEM. **CVE ID: CVE-2024-8441**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/236
Missing Authentication for Critical Function	10-Sep-2024	5.3	Missing authentication in Network Isolation of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to spoof Network Isolation status of managed devices. **CVE ID: CVE-2024-8320**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/237
Affected Version(s): 2024					
Improper Neutralization of Special Elements used in an	10-Sep-2024	9.8	SQL injection in the management console of Ivanti EPM before 2022 SU6, or the 2024 September update	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-	A-IVA-ENDP-180924/238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			allows a remote unauthenticated attacker to achieve remote code execution. **CVE ID: CVE-2024-8191**	2024-and-EPM-2022	
Deserialization of Untrusted Data	12-Sep-2024	9.8	Deserialization of untrusted data in the agent portal of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to achieve remote code execution. **CVE ID: CVE-2024-29847**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/239
N/A	10-Sep-2024	8.8	Weak authentication in Patch Management of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker to access restricted functionality. **CVE ID: CVE-2024-8322**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/240
Missing Authentication for Critical Function	10-Sep-2024	8.6	Missing authentication in Network Isolation of Ivanti EPM before 2022 SU6, or the 2024 September update	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-	A-IVA-ENDP-180924/241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to isolate managed devices from the network. **CVE ID: CVE-2024-8321**	2024-and-EPM-2022	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-32840**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/242
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-32842**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/243
Improper Neutralization of Special Elements used in an SQL Command	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			achieve remote code execution. **CVE ID: CVE-2024-32843**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-32845**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/245
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-32846**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/246
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/247

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
			CVE ID: CVE-2024-32848		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-34779**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/248
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-34783**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/249
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.2	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution. **CVE ID: CVE-2024-34785**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Search Path Element	10-Sep-2024	6.7	An uncontrolled search path in the agent of Ivanti EPM before 2022 SU6, or the 2024 September update allows a local authenticated attacker with admin privileges to escalate their privileges to SYSTEM. **CVE ID: CVE-2024-8441**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/251
Missing Authentication for Critical Function	10-Sep-2024	5.3	Missing authentication in Network Isolation of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to spoof Network Isolation status of managed devices. **CVE ID: CVE-2024-8320**	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022	A-IVA-ENDP-180924/252
Vendor: ivorysearch					
Product: ivory_search					
Affected Version(s): * Up to (excluding) 5.5.7					
N/A	05-Sep-2024	5.3	The Ivory Search – WordPress Search Plugin plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 5.5.6 via	https://plugins.trac.wordpress.org/changeset/3145289/	A-IVO-IVOR-180924/253

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 ajax_load_posts function. This makes it possible for unauthenticated attackers to extract text data from password-protected posts using the boolean-based attack on the AJAX search form **CVE ID: CVE-2024-6835**		
Vendor: kanev					
Product: cab_fare_calculator					
Affected Version(s): * Up to (including) 1.1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Sep-2024	4.8	The Cab fare calculator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the vehicle title setting in versions up to, and including, 1.1.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with administrative privileges to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-	N/A	A-KAN-CAB_-180924/254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			site installations and installations where unfiltered_html has been disabled. **CVE ID: CVE-2022-3556**		
Vendor: learningdigital					
Product: orca_hcm					
Affected Version(s): * Up to (excluding) 11.0					
N/A	09-Sep-2024	9.8	Orca HCM from LEARNING DIGITAL does not properly restrict access to a specific functionality, allowing unauthenticated remote attacker to exploit this functionality to create an account with administrator privilege and subsequently use it to log in. (The vendor is currently addressing the vulnerability. Once the fix is completed, we will provide information on the affected versions.) **CVE ID: CVE-2024-8584**	N/A	A-LEA-ORCA-180924/255
Improper Limitation of a Pathname to a Restricted Directory	09-Sep-2024	6.5	Orca HCM from LEARNING DIGITA does not properly restrict a specific parameter of the file download functionality,	N/A	A-LEA-ORCA-180924/256

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
('Path Traversal')			allowing a remote attacker with regular privileges to download arbitrary system files. **CVE ID: CVE-2024-8585**		
Vendor: lifterlms					
Product: lifterlms					
Affected Version(s): * Up to (excluding) 7.7.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Sep-2024	7.2	The LifterLMS – WP LMS for eLearning, Online Courses, & Quizzes plugin for WordPress is vulnerable to blind SQL Injection via the 'order' parameter in all versions up to, and including, 7.7.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive	https://plugins.trac.wordpress.org/changeset/3139798/lifterlms/tags/7.7.6/includes/abstracts/abstract.llms.database.query.php	A-LIF-LIFT-180924/257

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
			information from the database. **CVE ID: CVE-2024-7349**		
Vendor: Limesurvey					
Product: limesurvey					
Affected Version(s): * Up to (including) 6.6.1\\+240806					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Sep-2024	6.5	A Host header injection vulnerability in the password reset function of LimeSurvey v.6.6.1+240806 and before allows attackers to send users a crafted password reset link that will direct victims to a malicious domain. **CVE ID: CVE-2024-42903**	https://github.com/LimeSurvey/LimeSurvey/compare/6.6.0+240729...6.6.1+240806	A-LIM-LIME-180924/258
Vendor: linen					
Product: linen					
Affected Version(s): * Up to (excluding) 2024-04-03					
N/A	02-Sep-2024	9.8	Linen before cd37c3e does not verify that the domain is linen.dev or www.linen.dev when resetting a password. This occurs in create in apps/web/pages/api/forgot-password/index.ts. **CVE ID: CVE-2024-45522**	https://github.com/Linen-dev/linen.dev/commit/cd37c3e88ec29f4e7baae7e32fe80d0137848d10	A-LIN-LINE-180924/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Linuxfoundation					
Product: yocto					
Affected Version(s): 2.6					
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558; Issue ID: MSV-1526. **CVE ID: CVE-2024-20089**	https://corp.mediatek.com/product-security-bulletin/September-2024	A-LIN-YOCT-180924/260
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	A-LIN-YOCT-180924/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	A-LIN-YOCT-180924/262
Affected Version(s): 3.3					
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558; Issue ID: MSV-1526. **CVE ID: CVE-2024-20089**	https://corp.mediatek.com/product-security-bulletin/September-2024	A-LIN-YOCT-180924/263
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	A-LIN-YOCT-180924/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	bulletin/September-2024	
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	A-LIN-YOCT-180924/265
Affected Version(s): 4.0					
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional	https://corp.mediatek.com/product-security-bulletin/September-2024	A-LIN-YOCT-180924/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558; Issue ID: MSV-1526. **CVE ID: CVE-2024-20089**		
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	A-LIN-YOCT-180924/267
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204;	https://corp.mediatek.com/product-security-bulletin/September-2024	A-LIN-YOCT-180924/268

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
			Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Vendor: linuxos					
Product: shakal-ng					
Affected Version(s): * Up to (including) 1.3.3					
URL Redirection to Untrusted Site ('Open Redirect')	04-Sep-2024	6.1	A vulnerability, which was classified as problematic, was found in LinuxOSsk Shakal-NG up to 1.3.3. Affected is an unknown function of the file comments/views.py. The manipulation of the argument next leads to open redirect. It is possible to launch the attack remotely. The name of the patch is ebd1c2cba59cbac198bf2fd5a105659944d4f02cb. It is recommended to apply a patch to fix this issue. **CVE ID: CVE-2024-8412**	https://github.com/LinuxOSsk/Shakal-NG/commit/ebd1c2cba59cbac198bf2fd5a10565994d4f02cb	A-LIN-SHAK-180924/269
Vendor: loway					
Product: queuemetrics					
Affected Version(s): From (including) 17.06.1 Up to (excluding) 24.05.5					
Observable Discrepancy	08-Sep-2024	7.5	Loway - CWE-204: Observable	N/A	A-LOW-QUEU-180924/270

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
			Response Discrepancy **CVE ID: CVE-2024-42343**		
Affected Version(s): From (including) 22.11.6 Up to (excluding) 24.05.5					
URL Redirection to Untrusted Site ('Open Redirect')	08-Sep-2024	6.1	Loway - CWE-601: URL Redirection to Untrusted Site ('Open Redirect') **CVE ID: CVE-2024-42341**	N/A	A-LOW-QUEU-180924/271
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	08-Sep-2024	4.3	Loway - CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') **CVE ID: CVE-2024-42342**	N/A	A-LOW-QUEU-180924/272
Vendor: majeedraza					
Product: carousel_slider					
Affected Version(s): * Up to (excluding) 2.0					
Cross-Site Request Forgery (CSRF)	02-Sep-2024	4.3	WordPress plugin "Carousel Slider" provided by Sayful Islam contains a cross-site request forgery vulnerability on Carousel image selection feature. While logged in to the WordPress site with Carousel Slider plugin enabled, accessing a crafted page may cause a user to alter	N/A	A-MAJ-CARO-180924/273

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 contents of the WordPress site. **CVE ID: CVE-2024-45269**		
Affected Version(s): * Up to (excluding) 2.2.4					
Cross-Site Request Forgery (CSRF)	02-Sep-2024	4.3	WordPress plugin "Carousel Slider" provided by Sayful Islam contains a cross-site request forgery vulnerability on Hero image selection feature. While logged in to the WordPress site with Carousel Slider plugin enabled, accessing a crafted page may cause a user to alter the contents of the WordPress site. **CVE ID: CVE-2024-45270**	N/A	A-MAJ-CARO-180924/274
Vendor: mayurik					
Product: best_house_rental_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	8.8	A vulnerability classified as critical has been found in SourceCodester Best House Rental Management System 1.0. Affected is the function delete_user/save_user of the file /admin_class.php. The manipulation	N/A	A-MAY-BEST-180924/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2024-8709**		
Vendor: Microsoft					
Product: 365_apps					
Affected Version(s): -					
N/A	10-Sep-2024	7.8	Microsoft Excel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-43465**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43465	A-MIC-365_-180924/276
Product: dynamics_365					
Affected Version(s): * Up to (excluding) 9.1.32					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Sep-2024	5.4	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID: CVE-2024-43476**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43476	A-MIC-DYNA-180924/277
Product: excel					
Affected Version(s): 2016					
N/A	10-Sep-2024	7.8	Microsoft Excel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-43465**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43465	A-MIC-EXCE-180924/278

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
Product: office					
Affected Version(s): 2021					
N/A	10-Sep-2024	7.3	Microsoft Publisher Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38226**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38226	A-MIC-OFFI-180924/279
Affected Version(s): 2019					
N/A	10-Sep-2024	7.8	Microsoft Excel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-43465**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43465	A-MIC-OFFI-180924/280
N/A	10-Sep-2024	7.3	Microsoft Publisher Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38226**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38226	A-MIC-OFFI-180924/281
Product: office_long_term_servicing_channel					
Affected Version(s): 2021					
N/A	10-Sep-2024	7.8	Microsoft Excel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-43465**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43465	A-MIC-OFFI-180924/282
Product: office_online_server					
Affected Version(s): * Up to (excluding) 16.0.10414.20000					
N/A	10-Sep-2024	7.8	Microsoft Excel Elevation of Privilege Vulnerability **CVE ID: CVE-2024-43465**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43465	A-MIC-OFFI-180924/283
Product: power_automate					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 2.41 Up to (excluding) 2.41.178.24249					
N/A	10-Sep-2024	8.5	Microsoft Power Automate Desktop Remote Code Execution Vulnerability **CVE ID: CVE-2024-43479**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43479	A-MIC-POWE-180924/284
Affected Version(s): From (including) 2.42 Up to (excluding) 2.42.331.24249					
N/A	10-Sep-2024	8.5	Microsoft Power Automate Desktop Remote Code Execution Vulnerability **CVE ID: CVE-2024-43479**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43479	A-MIC-POWE-180924/285
Affected Version(s): From (including) 2.43 Up to (excluding) 2.43.249.24249					
N/A	10-Sep-2024	8.5	Microsoft Power Automate Desktop Remote Code Execution Vulnerability **CVE ID: CVE-2024-43479**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43479	A-MIC-POWE-180924/286
Affected Version(s): From (including) 2.44 Up to (excluding) 2.44.55.24249					
N/A	10-Sep-2024	8.5	Microsoft Power Automate Desktop Remote Code Execution Vulnerability **CVE ID: CVE-2024-43479**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43479	A-MIC-POWE-180924/287
Affected Version(s): From (including) 2.45 Up to (excluding) 2.45.404.24249					
N/A	10-Sep-2024	8.5	Microsoft Power Automate Desktop Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43479	A-MIC-POWE-180924/288

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
			CVE ID: CVE-2024-43479		
Affected Version(s): From (including) 2.46 Up to (excluding) 2.46.181.24249					
N/A	10-Sep-2024	8.5	Microsoft Power Automate Desktop Remote Code Execution Vulnerability **CVE ID: CVE-2024-43479**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43479	A-MIC-POWE-180924/289
Affected Version(s): From (including) 2.47 Up to (excluding) 2.47.119.24249					
N/A	10-Sep-2024	8.5	Microsoft Power Automate Desktop Remote Code Execution Vulnerability **CVE ID: CVE-2024-43479**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43479	A-MIC-POWE-180924/290
Product: publisher					
Affected Version(s): 2016					
N/A	10-Sep-2024	7.3	Microsoft Publisher Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38226**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38226	A-MIC-PUBL-180924/291
Product: sharepoint_server					
Affected Version(s): -					
N/A	10-Sep-2024	7.5	Microsoft SharePoint Server Denial of Service Vulnerability **CVE ID: CVE-2024-43466**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43466	A-MIC-SHAR-180924/292
N/A	10-Sep-2024	7.2	Microsoft SharePoint Server Remote Code	https://msrc.microsoft.com/update-guide/vulnerabi	A-MIC-SHAR-180924/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-43464**	lity/CVE-2024-43464	
Affected Version(s): 2016					
N/A	10-Sep-2024	7.5	Microsoft SharePoint Server Denial of Service Vulnerability **CVE ID: CVE-2024-43466**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43466	A-MIC-SHAR-180924/294
N/A	10-Sep-2024	7.2	Microsoft SharePoint Server Remote Code Execution Vulnerability **CVE ID: CVE-2024-43464**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43464	A-MIC-SHAR-180924/295
Affected Version(s): 2019					
N/A	10-Sep-2024	7.5	Microsoft SharePoint Server Denial of Service Vulnerability **CVE ID: CVE-2024-43466**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43466	A-MIC-SHAR-180924/296
N/A	10-Sep-2024	7.2	Microsoft SharePoint Server Remote Code Execution Vulnerability **CVE ID: CVE-2024-43464**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43464	A-MIC-SHAR-180924/297
Vendor: mindsdb					
Product: mindsdb					
Affected Version(s): *					
Improper Neutralization of Input During	12-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability exists in all versions of the	N/A	A-MIN-MIND-180924/298

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
Web Page Generation ('Cross-site Scripting')			MindsDB platform, enabling the execution of a JavaScript payload whenever a user enumerates an ML Engine, database, project, or dataset containing arbitrary JavaScript code within the web UI. **CVE ID: CVE-2024-45856**		
Affected Version(s): * Up to (excluding) 23.12.4.2					
Server-Side Request Forgery (SSRF)	05-Sep-2024	9.1	MindsDB is a platform for building artificial intelligence from enterprise data. Prior to version 23.12.4.2, a threat actor can bypass the server-side request forgery protection on the whole website with DNS Rebinding. The vulnerability can also lead to denial of service. Version 23.12.4.2 contains a patch. **CVE ID: CVE-2024-24759**	https://github.com/mindsdb/mindsdb/commit/5f7496481bd3db1d06a2d2e62c0dce960a1fe12b, https://github.com/mindsdb/mindsdb/security/advisories/GHSA-4jcv-vp96-94xr	A-MIN-MIND-180924/299
Affected Version(s): From (including) 23.10.3.0 Up to (excluding) 24.7.4.1					
Improper Control of Generation of Code ('Code Injection')	12-Sep-2024	8.8	An arbitrary code execution vulnerability exists in versions 23.10.3.0 up to 24.7.4.1 of the	N/A	A-MIN-MIND-180924/300

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
			MindsDB platform, when the Weaviate integration is installed on the server. If a specially crafted 'SELECT WHERE' clause containing Python code is run against a database created with the Weaviate engine, the code will be passed to an eval function and executed on the server. **CVE ID: CVE-2024-45846**		
Affected Version(s): From (including) 23.10.5.0 Up to (excluding) 24.7.4.1					
Improper Control of Generation of Code ('Code Injection')	12-Sep-2024	8.8	An arbitrary code execution vulnerability exists in versions 23.10.5.0 up to 24.7.4.1 of the MindsDB platform, when the Microsoft SharePoint integration is installed on the server. For databases created with the SharePoint engine, an 'INSERT' query can be used for list creation. If such a query is specially crafted to contain Python code and is run against the database, the code will be passed to an	N/A	A-MIN-MIND-180924/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			eval function and executed on the server. **CVE ID: CVE-2024-45849**		
Improper Control of Generation of Code ('Code Injection')	12-Sep-2024	8.8	An arbitrary code execution vulnerability exists in versions 23.10.5.0 up to 24.7.4.1 of the MindsDB platform, when the Microsoft SharePoint integration is installed on the server. For databases created with the SharePoint engine, an 'INSERT' query can be used for site column creation. If such a query is specially crafted to contain Python code and is run against the database, the code will be passed to an eval function and executed on the server. **CVE ID: CVE-2024-45850**	N/A	A-MIN-MIND-180924/302
Improper Control of Generation of Code ('Code Injection')	12-Sep-2024	8.8	An arbitrary code execution vulnerability exists in versions 23.10.5.0 up to 24.7.4.1 of the MindsDB platform, when the Microsoft SharePoint	N/A	A-MIN-MIND-180924/303

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
			integration is installed on the server. For databases created with the SharePoint engine, an 'INSERT' query can be used for list item creation. If such a query is specially crafted to contain Python code and is run against the database, the code will be passed to an eval function and executed on the server. **CVE ID: CVE-2024-45851**		
Affected Version(s): From (including) 23.11.4.2 Up to (excluding) 24.7.4.1					
Improper Control of Generation of Code ('Code Injection')	12-Sep-2024	8.8	An arbitrary code execution vulnerability exists in versions 23.11.4.2 up to 24.7.4.1 of the MindsDB platform, when one of several integrations is installed on the server. If a specially crafted 'UPDATE' query containing Python code is run against a database created with the specified integration engine, the code will be passed to an eval function and	N/A	A-MIN-MIND-180924/304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed on the server. **CVE ID: CVE-2024-45847**		
Affected Version(s): From (including) 23.12.4.0 Up to (excluding) 24.7.4.1					
Improper Control of Generation of Code ('Code Injection')	12-Sep-2024	8.8	An arbitrary code execution vulnerability exists in versions 23.12.4.0 up to 24.7.4.1 of the MindsDB platform, when the ChromaDB integration is installed on the server. If a specially crafted 'INSERT' query containing Python code is run against a database created with the ChromaDB engine, the code will be passed to an eval function and executed on the server. **CVE ID: CVE-2024-45848**	N/A	A-MIN-MIND-180924/305
Vendor: Misp					
Product: misp					
Affected Version(s): * Up to (excluding) 2.4.197					
Incorrect Authorization	01-Sep-2024	6.5	In MISP through 2.4.196, app/Controller/BookmarksController.php does not properly restrict access to bookmarks data in	https://github.com/MISP/MISP/commit/3f3b9a574f349182a545636e12efa39267e9db04	A-MIS-MISP-180924/306

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 case where the user is not an org admin. **CVE ID: CVE-2024-45509**		
Vendor: Mozilla					
Product: firefox					
Affected Version(s): * Up to (excluding) 130.0					
Access of Resource Using Incompatible Type ('Type Confusion')	03-Sep-2024	9.8	A potentially exploitable type confusion could be triggered when looking up a property name on an object being used as the `with` environment. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, Firefox ESR < 115.15, Thunderbird < 128.2, and Thunderbird < 115.15. **CVE ID: CVE-2024-8381**	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/, https://www.mozilla.org/security/advisories/mfsa2024-41/	A-MOZ-FIRE-180924/307
Out-of-bounds Write	03-Sep-2024	9.8	The JavaScript garbage collector could mis-color cross-compartment objects if OOM conditions were detected at the right point between two passes. This could have led to memory corruption. This vulnerability	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/, https://www.mozilla.org/security/advisories/mfsa2024-41/	A-MOZ-FIRE-180924/308

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
			affects Firefox < 130, Firefox ESR < 128.2, Firefox ESR < 115.15, Thunderbird < 128.2, and Thunderbird < 115.15. **CVE ID: CVE-2024-8384**		
Access of Resource Using Incompatible Type ('Type Confusion')	03-Sep-2024	9.8	A difference in the handling of StructFields and ArrayTypes in WASM could be used to trigger an exploitable type confusion vulnerability. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, and Thunderbird < 128.2. **CVE ID: CVE-2024-8385**	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/	A-MOZ-FIRE-180924/309
N/A	03-Sep-2024	8.8	Internal browser event interfaces were exposed to web content when privileged EventHandler listener callbacks ran for those events. Web content that tried to use those interfaces would not be able to use them with elevated privileges, but their presence would	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/, https://www.mozilla.org/security/advisories/mfsa2024-41/	A-MOZ-FIRE-180924/310

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
			indicate certain browser features had been used, such as when a user opened the Dev Tools console. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, Firefox ESR < 115.15, Thunderbird < 128.2, and Thunderbird < 115.15. **CVE ID: CVE-2024-8382**		
N/A	03-Sep-2024	7.5	Firefox normally asks for confirmation before asking the operating system to find an application to handle a scheme that the browser does not support. It did not ask before doing so for the Usenet-related schemes news: and snews:. Since most operating systems don't have a trusted newsreader installed by default, an unscrupulous program that the user downloaded could register itself as a handler. The website that served the application download could	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/, https://www.mozilla.org/security/advisories/mfsa2024-41/	A-MOZ-FIRE-180924/311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			then launch that application at will. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, and Firefox ESR < 115.15. **CVE ID: CVE-2024-8383**		
URL Redirection to Untrusted Site ('Open Redirect')	03-Sep-2024	6.1	If a site had been granted the permission to open popup windows, it could cause Select elements to appear on top of another site to perform a spoofing attack. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, and Thunderbird < 128.2. **CVE ID: CVE-2024-8386**	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/	A-MOZ-FIRE-180924/312
N/A	03-Sep-2024	5.3	Multiple prompts and panels from both Firefox and the Android OS could be used to obscure the notification announcing the transition to fullscreen mode after the fix for CVE-2023-6870 in Firefox 121. This could lead to spoofing the browser UI if the sudden appearance	https://www.mozilla.org/security/advisories/mfsa2024-39/	A-MOZ-FIRE-180924/313

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the prompt distracted the user from noticing the visual transition happening behind the prompt. These notifications now use the Android Toast feature. *This bug only affects Firefox on Android. Other operating systems are unaffected.* This vulnerability affects Firefox < 130. **CVE ID: CVE-2024-8388**		
Affected Version(s): 129.0					
Out-of-bounds Write	03-Sep-2024	9.8	Memory safety bugs present in Firefox 129, Firefox ESR 128.1, and Thunderbird 128.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, and Thunderbird < 128.2. **CVE ID: CVE-2024-8387**	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/	A-MOZ-FIRE-180924/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	03-Sep-2024	9.8	Memory safety bugs present in Firefox 129. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 130. **CVE ID: CVE-2024-8389**	https://www.mozilla.org/security/advisories/mfsa2024-39/	A-MOZ-FIRE-180924/315
Product: firefox_esr					
Affected Version(s): * Up to (excluding) 115.15					
Access of Resource Using Incompatible Type ('Type Confusion')	03-Sep-2024	9.8	A potentially exploitable type confusion could be triggered when looking up a property name on an object being used as the `with` environment. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, Firefox ESR < 115.15, Thunderbird < 128.2, and Thunderbird < 115.15. **CVE ID: CVE-2024-8381**	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/, https://www.mozilla.org/security/advisories/mfsa2024-41/	A-MOZ-FIRE-180924/316
Out-of-bounds Write	03-Sep-2024	9.8	The JavaScript garbage collector could mis-color	https://www.mozilla.org/security/advisories/	A-MOZ-FIRE-180924/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cross-compartment objects if OOM conditions were detected at the right point between two passes. This could have led to memory corruption. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, Firefox ESR < 115.15, Thunderbird < 128.2, and Thunderbird < 115.15. **CVE ID: CVE-2024-8384**	mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/, https://www.mozilla.org/security/advisories/mfsa2024-41/	
N/A	03-Sep-2024	8.8	Internal browser event interfaces were exposed to web content when privileged EventHandler listener callbacks ran for those events. Web content that tried to use those interfaces would not be able to use them with elevated privileges, but their presence would indicate certain browser features had been used, such as when a user opened the Dev Tools console. This	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/, https://www.mozilla.org/security/advisories/mfsa2024-41/	A-MOZ-FIRE-180924/318

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
			vulnerability affects Firefox < 130, Firefox ESR < 128.2, Firefox ESR < 115.15, Thunderbird < 128.2, and Thunderbird < 115.15. **CVE ID: CVE-2024-8382**		
N/A	03-Sep-2024	7.5	Firefox normally asks for confirmation before asking the operating system to find an application to handle a scheme that the browser does not support. It did not ask before doing so for the Usenet-related schemes news: and snews:. Since most operating systems don't have a trusted newsreader installed by default, an unscrupulous program that the user downloaded could register itself as a handler. The website that served the application download could then launch that application at will. This vulnerability affects Firefox < 130, Firefox ESR <	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/, https://www.mozilla.org/security/advisories/mfsa2024-41/	A-MOZ-FIRE-180924/319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			128.2, and Firefox ESR < 115.15. **CVE ID: CVE-2024-8383**		
Affected Version(s): * Up to (excluding) 128.2					
Access of Resource Using Incompatible Type ('Type Confusion')	03-Sep-2024	9.8	A difference in the handling of StructFields and ArrayTypes in WASM could be used to trigger an exploitable type confusion vulnerability. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, and Thunderbird < 128.2. **CVE ID: CVE-2024-8385**	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/	A-MOZ-FIRE-180924/320
URL Redirection to Untrusted Site ('Open Redirect')	03-Sep-2024	6.1	If a site had been granted the permission to open popup windows, it could cause Select elements to appear on top of another site to perform a spoofing attack. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, and Thunderbird < 128.2. **CVE ID: CVE-2024-8386**	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/	A-MOZ-FIRE-180924/321
Affected Version(s): 128.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	03-Sep-2024	9.8	Memory safety bugs present in Firefox 129, Firefox ESR 128.1, and Thunderbird 128.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, and Thunderbird < 128.2. **CVE ID: CVE-2024-8387**	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/	A-MOZ-FIRE-180924/322
Affected Version(s): From (including) 128.0 Up to (excluding) 128.2					
Access of Resource Using Incompatible Type ('Type Confusion')	03-Sep-2024	9.8	A potentially exploitable type confusion could be triggered when looking up a property name on an object being used as the `with` environment. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, Firefox ESR < 115.15, Thunderbird < 128.2, and Thunderbird < 115.15.	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/, https://www.mozilla.org/security/advisories/mfsa2024-41/	A-MOZ-FIRE-180924/323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8381		
Out-of-bounds Write	03-Sep-2024	9.8	The JavaScript garbage collector could mis-color cross-compartment objects if OOM conditions were detected at the right point between two passes. This could have led to memory corruption. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, Firefox ESR < 115.15, Thunderbird < 128.2, and Thunderbird < 115.15. **CVE ID: CVE-2024-8384**	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/, https://www.mozilla.org/security/advisories/mfsa2024-41/	A-MOZ-FIRE-180924/324
N/A	03-Sep-2024	8.8	Internal browser event interfaces were exposed to web content when privileged EventHandler listener callbacks ran for those events. Web content that tried to use those interfaces would not be able to use them with elevated privileges, but their presence would indicate certain	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/, https://www.mozilla.org/security/advisories/mfsa2024-41/	A-MOZ-FIRE-180924/325

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
			browser features had been used, such as when a user opened the Dev Tools console. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, Firefox ESR < 115.15, Thunderbird < 128.2, and Thunderbird < 115.15. **CVE ID: CVE-2024-8382**		
N/A	03-Sep-2024	7.5	Firefox normally asks for confirmation before asking the operating system to find an application to handle a scheme that the browser does not support. It did not ask before doing so for the Usenet-related schemes news: and snews:. Since most operating systems don't have a trusted newsreader installed by default, an unscrupulous program that the user downloaded could register itself as a handler. The website that served the application download could then launch that	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/, https://www.mozilla.org/security/advisories/mfsa2024-41/	A-MOZ-FIRE-180924/326

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
			application at will. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, and Firefox ESR < 115.15. **CVE ID: CVE-2024-8383**		
Product: firefox_focus					
Affected Version(s): * Up to (excluding) 130.0					
N/A	03-Sep-2024	4.7	Websites could utilize Javascript links to spoof URL addresses in the Focus navigation bar This vulnerability affects Focus for iOS < 130. **CVE ID: CVE-2024-8399**	https://www.mozilla.org/security/advisories/mfsa2024-42/	A-MOZ-FIRE-180924/327
Product: thunderbird					
Affected Version(s): 128.1					
Out-of-bounds Write	03-Sep-2024	9.8	Memory safety bugs present in Firefox 129, Firefox ESR 128.1, and Thunderbird 128.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, and	https://www.mozilla.org/security/advisories/mfsa2024-39/, https://www.mozilla.org/security/advisories/mfsa2024-40/	A-MOZ-THUN-180924/328

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
			Thunderbird < 128.2. **CVE ID: CVE-2024-8387**		
Affected Version(s): * Up to (excluding) 128.2.0					
Use After Free	06-Sep-2024	6.5	When aborting the verification of an OTR chat session, an attacker could have caused a use-after-free bug leading to a potentially exploitable crash. This vulnerability affects Thunderbird < 128.2. **CVE ID: CVE-2024-8394**	https://www.mozilla.org/security/advisories/mfsa2024-43/	A-MOZ-THUN-180924/329
Vendor: Mozilo					
Product: mozilocms					
Affected Version(s): 3.0					
Unrestricted Upload of File with Dangerous Type	10-Sep-2024	7.2	An arbitrary file upload vulnerability in the component /admin/index.php of moziloCMS v3.0 allows attackers to execute arbitrary code via uploading a crafted file. **CVE ID: CVE-2024-44871**	N/A	A-MOZ-MOZI-180924/330
Improper Neutralization of Input During Web Page	10-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in moziloCMS v3.0 allows attackers to	N/A	A-MOZ-MOZI-180924/331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			execute arbitrary code in the context of a user's browser via injecting a crafted payload. **CVE ID: CVE-2024-44872**		
Vendor: msoftplugins					
Product: security_antivirus_firewall					
Affected Version(s): * Up to (including) 2.3.5					
N/A	05-Sep-2024	5.3	The Security, Antivirus, Firewall – S.A.F plugin for WordPress is vulnerable to IP Address Spoofing in versions up to, and including, 2.3.5. This is due to insufficient restrictions on where the IP Address information is being retrieved for request logging and login restrictions. Attackers can supply the X-Forwarded-For header with with a different IP Address that will be logged and can be used to bypass settings that may have blocked out an IP address from logging in. **CVE ID: CVE-2022-4529**	N/A	A-MSO-SECU-180924/332

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
Vendor: multivendorx					
Product: multivendorx					
Affected Version(s): * Up to (excluding) 4.2.1					
Missing Authorization	04-Sep-2024	9.8	The MultiVendorX – The Ultimate WooCommerce Multivendor Marketplace Solution plugin for WordPress is vulnerable to privilege escalation/de-escalation and account takeover due to an insufficient capability check on the update_item_permissions_check and create_item_permissions_check functions in all versions up to, and including, 4.2.0. This makes it possible for unauthenticated attackers to change the password of any user with the vendor role, create new users with the vendor role, and demote other users like administrators to the vendor role. **CVE ID: CVE-2024-8289**	N/A	A-MUL-MULT-180924/333
Vendor: munyweki					
Product: insurance_management_system					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0					
Cross-Site Request Forgery (CSRF)	04-Sep-2024	4.3	A vulnerability has been found in SourceCodester Insurance Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality. 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-2024-8414**	N/A	A-MUN-INSU-180924/334
Vendor: nescalante					
Product: urlregex					
Affected Version(s): * Up to (excluding) 0.5.1					
N/A	02-Sep-2024	7.5	A vulnerability was found in nescalante urlregex up to 0.5.0 and classified as problematic. This issue affects some unknown processing of the file index.js of the component Backtracking. The manipulation leads to inefficient regular expression complexity. The	https://github.com/nescalante/urlregex/commit/e5a085afe6abfaea1d1a78f54c45af9ef43ca1f9	A-NES-URLR-180924/335

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
			attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 0.5.1 is able to address this issue. The identifier of the patch is e5a085afe6abfaea1d1a78f54c45af9ef43ca1f9. It is recommended to upgrade the affected component. **CVE ID: CVE-2020-36830**		
Vendor: ngothang					
Product: wp_multitasking					
Affected Version(s): * Up to (including) 0.1.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Sep-2024	5.4	The WP MultiTasking WordPress plugin through 0.1.12 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	N/A	A-NGO-WP_M-180924/336

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
			CVE ID: CVE-2024-6859		
Cross-Site Request Forgery (CSRF)	08-Sep-2024	4.3	The WP MultiTasking WordPress plugin through 0.1.12 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack **CVE ID: CVE-2024-6852**	N/A	A-NGO-WP_M-180924/337
Cross-Site Request Forgery (CSRF)	08-Sep-2024	4.3	The WP MultiTasking WordPress plugin through 0.1.12 does not have CSRF check when updating welcome popups, which could allow attackers to make logged admins perform such action via a CSRF attack **CVE ID: CVE-2024-6853**	N/A	A-NGO-WP_M-180924/338
Cross-Site Request Forgery (CSRF)	08-Sep-2024	4.3	The WP MultiTasking WordPress plugin through 0.1.12 does not have CSRF check when updating exit popups, which could allow	N/A	A-NGO-WP_M-180924/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to make logged admins perform such action via a CSRF attack **CVE ID: CVE-2024-6855**		
Cross-Site Request Forgery (CSRF)	08-Sep-2024	4.3	The WP MultiTasking WordPress plugin through 0.1.12 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack **CVE ID: CVE-2024-6856**	N/A	A-NGO-WP_M-180924/340
Vendor: onesoftnet					
Product: sudobot					
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.26.7					
Missing Authorization	03-Sep-2024	9.8	SudoBot, a Discord moderation bot, is vulnerable to privilege escalation and exploit of the `-config` command in versions prior to 9.26.7. Anyone is theoretically able to update any configuration of the bot and potentially gain control over the bot's settings. Every version of v9 before v9.26.7 is affected. Other	https://github.com/onesoft-sudo/sudobot/commit/ef46ca98562f3c1abef4ff7dd94d8f7b8155ee50, https://github.com/onesoft-sudo/sudobot/security/advisories/GHSA-crgg-w3rr-r9h4	A-ONE-SUDO-180924/341

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
			versions (e.g. v8) are not affected. Users should upgrade to version 9.26.7 to receive a patch. A workaround would be to create a command permission overwrite in the Database. A SQL statement provided in the GitHub Security Advisor can be executed to create a overwrite that disallows users without `ManageGuild` permission to run the `-config` command. Run the SQL statement for every server the bot is in, and replace `<guild_id>` with the appropriate Guild ID each time. **CVE ID: CVE-2024-45307**		
Vendor: online_food_ordering_system_project					
Product: online_food_ordering_system					
Affected Version(s): 2.0					
Improper Neutralization of Input During Web Page Generation	09-Sep-2024	6.1	A vulnerability classified as problematic has been found in SourceCodester Online Food Ordering System	N/A	A-ONL-ONLI-180924/342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			2.0. This affects an unknown part of the file index.php of the component Create an Account Page. The manipulation of the argument First Name/Last Name leads to cross site scripting. It is possible to initiate the attack remotely. **CVE ID: CVE-2024-8604**		
Vendor: online_shop_store_project					
Product: online_shop_store					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Sep-2024	6.1	A vulnerability classified as problematic was found in code-projects Online Shop Store 1.0. This vulnerability affects unknown code of the file /settings.php. The manipulation of the argument error leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8566**	N/A	A-ONL-ONLI-180924/343

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
Vendor: opensc_project					
Product: opensc					
Affected Version(s): * Up to (excluding) 0.26.0					
Use of Uninitialized Resource	03-Sep-2024	3.9	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK. The problem is missing initialization of variables expected to be initialized (as arguments to other functions, etc.). **CVE ID: CVE-2024-45615**	https://access.redhat.com/security/cve/CVE-2024-45615, https://bugzilla.redhat.com/show_bug.cgi?id=2309285	A-OPE-OPEN-180924/344
Use of Uninitialized Resource	03-Sep-2024	3.9	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. The following problems were caused by insufficient control of the response APDU buffer and its length when communicating with the card.	https://access.redhat.com/security/cve/CVE-2024-45616, https://bugzilla.redhat.com/show_bug.cgi?id=2309290	A-OPE-OPEN-180924/345

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
			CVE ID: CVE-2024-45616		
Use of Uninitialized Resource	03-Sep-2024	3.9	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. Insufficient or missing checking of return values of functions leads to unexpected work with variables that have not been initialized. **CVE ID: CVE-2024-45617**	https://access.redhat.com/security/cve/CVE-2024-45617, https://bugzilla.redhat.com/show_bug.cgi?id=2309286	A-OPE-OPEN-180924/346
Use of Uninitialized Resource	03-Sep-2024	3.9	A vulnerability was found in pkcs15-init in OpenSC. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. Insufficient or missing checking of return values of functions leads to	https://access.redhat.com/security/cve/CVE-2024-45618, https://bugzilla.redhat.com/show_bug.cgi?id=2309287	A-OPE-OPEN-180924/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpected work with variables that have not been initialized. **CVE ID: CVE-2024-45618**		
Vendor: oretnom23					
Product: clinic\'s_patient_management_system					
Affected Version(s): 2.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Sep-2024	9.8	A vulnerability was found in SourceCodesters Clinics Patient Management System 2.0. It has been rated as critical. This issue affects some unknown processing of the file /print_diseases.php. The manipulation of the argument disease/from/to 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-2024-8565**	N/A	A-ORE-CLIN-180924/348
URL Redirection to Untrusted	07-Sep-2024	6.1	A vulnerability was found in SourceCodester Clinics Patient Management System 2.0. It has	N/A	A-ORE-CLIN-180924/349

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
Site ('Open Redirect')			been classified as problematic. Affected is an unknown function of the file congratulations.php. The manipulation of the argument goto_page leads to open redirect. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8555**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-2024	5.4	A vulnerability was found in SourceCodester Clinics Patient Management System 2.0 and classified as problematic. This issue affects some unknown processing of the file /users.php. The manipulation of the argument message leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	N/A	A-ORE-CLIN-180924/350

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
			CVE ID: CVE-2024-8554		
Product: food_ordering_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Sep-2024	9.8	A vulnerability was found in SourceCodester Food Ordering Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /routers/add-ticket.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-2024-8415**	N/A	A-ORE-FOOD-180924/351
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Sep-2024	9.8	A vulnerability was found in SourceCodester Food Ordering Management System 1.0. It has been classified as critical. This affects an unknown part of the file /routers/ticket-status.php. The manipulation of the argument ticket_id	N/A	A-ORE-FOOD-180924/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8416**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Sep-2024	7.5	A vulnerability classified as critical has been found in SourceCodester Food Ordering Management System 1.0. This affects an unknown part of the file /foms/routers/cancel-order.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8557**	N/A	A-ORE-FOOD-180924/353
N/A	12-Sep-2024	7.5	A vulnerability, which was classified as problematic, has been found in SourceCodester Food Ordering Management System 1.0.	N/A	A-ORE-FOOD-180924/354

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Affected by this issue is some unknown functionality of the file /includes/. The manipulation leads to exposure of information through directory listing. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8711**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Sep-2024	6.1	A vulnerability was found in SourceCodester Food Ordering 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 description 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-2024-8582**	N/A	A-ORE-FOOD-180924/355

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 Validation of Specified Quantity in Input	07-Sep-2024	4.3	A vulnerability classified as problematic was found in SourceCodester Food Ordering Management System 1.0. This vulnerability affects unknown code of the file /foms/routers/place-order.php of the component Price Handler. The manipulation of the argument total leads to improper validation of specified quantity in input. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8558**	N/A	A-ORE-FOOD-180924/356
Product: online_bank_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Sep-2024	5.4	A vulnerability was found in SourceCodester Online Bank Management System and Online Bank Management System - 1.0. It has been classified as problematic. This affects an unknown part of the file	N/A	A-ORE-ONLI-180924/357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/mfeedback.php of the component Feedback Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8583**		
Product: simple_invoice_generator_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Sep-2024	8.8	A vulnerability, which was classified as critical, was found in SourceCodester Simple Invoice Generator System 1.0. Affected is an unknown function of the file /save_invoice.php. The manipulation of the argument invoice_code/customer/cashier/total_amount/discount_percentage/discount_amount/tendered_amount leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the	N/A	A-ORE-SIMP-180924/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. **CVE ID: CVE-2024-8560**		
Vendor: overwolf					
Product: overwolf					
Affected Version(s): * Up to (excluding) 250.1.1					
Uncontrolled Search Path Element	04-Sep-2024	7.8	A local privilege escalation is caused by Overwolf loading and executing certain dynamic link library files from a user-writeable folder in SYSTEM context on launch. This allows an attacker with unprivileged access to the system to run arbitrary code with SYSTEM privileges by placing a malicious .dll file in the respective location. **CVE ID: CVE-2024-7834**	N/A	A-OVE-OVER-180924/359
Vendor: payara					
Product: payara					
Affected Version(s): From (including) 4.1.2.191.0 Up to (excluding) 4.1.2.191.50					
URL Redirection to Untrusted Site ('Open Redirect')	11-Sep-2024	6.1	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Payara Platform Payara Server	N/A	A-PAY-PAYA-180924/360

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
			(REST Management Interface modules) allows Session Hijacking.This issue affects Payara Server: from 6.0.0 before 6.18.0, from 6.2022.1 before 6.2024.9, from 5.2020.2 before 5.2022.5, from 5.20.0 before 5.67.0, from 4.1.2.191.0 before 4.1.2.191.50. **CVE ID: CVE-2024-7312**		
Affected Version(s): From (including) 5.20.0 Up to (excluding) 5.67.0					
URL Redirection to Untrusted Site ('Open Redirect')	11-Sep-2024	6.1	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Payara Platform Payara Server (REST Management Interface modules) allows Session Hijacking.This issue affects Payara Server: from 6.0.0 before 6.18.0, from 6.2022.1 before 6.2024.9, from 5.2020.2 before 5.2022.5, from 5.20.0 before 5.67.0, from 4.1.2.191.0 before 4.1.2.191.50. **CVE ID: CVE-2024-7312**	N/A	A-PAY-PAYA-180924/361
Affected Version(s): From (including) 5.2020.2 Up to (excluding) 5.2022.5					

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
URL Redirection to Untrusted Site ('Open Redirect')	11-Sep-2024	6.1	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Payara Platform Payara Server (REST Management Interface modules) allows Session Hijacking.This issue affects Payara Server: from 6.0.0 before 6.18.0, from 6.2022.1 before 6.2024.9, from 5.2020.2 before 5.2022.5, from 5.20.0 before 5.67.0, from 4.1.2.191.0 before 4.1.2.191.50. **CVE ID: CVE-2024-7312**	N/A	A-PAY-PAYA-180924/362
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.18.0					
URL Redirection to Untrusted Site ('Open Redirect')	11-Sep-2024	6.1	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Payara Platform Payara Server (REST Management Interface modules) allows Session Hijacking.This issue affects Payara Server: from 6.0.0 before 6.18.0, from 6.2022.1 before 6.2024.9, from 5.2020.2 before 5.2022.5, from 5.20.0 before 5.67.0, from	N/A	A-PAY-PAYA-180924/363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4.1.2.191.0 before 4.1.2.191.50. **CVE ID: CVE-2024-7312**		
Affected Version(s): From (including) 6.2022.1 Up to (excluding) 6.2024.9					
URL Redirection to Untrusted Site ('Open Redirect')	11-Sep-2024	6.1	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Payara Platform Payara Server (REST Management Interface modules) allows Session Hijacking.This issue affects Payara Server: from 6.0.0 before 6.18.0, from 6.2022.1 before 6.2024.9, from 5.2020.2 before 5.2022.5, from 5.20.0 before 5.67.0, from 4.1.2.191.0 before 4.1.2.191.50. **CVE ID: CVE-2024-7312**	N/A	A-PAY-PAYA-180924/364
Vendor: payroll_management_system_project					
Product: payroll_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Sep-2024	9.8	A vulnerability, which was classified as critical, has been found in itsourcecode Payroll Management System 1.0. This issue affects some unknown	N/A	A-PAY-PAYR-180924/365

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
			processing of the file /ajax.php?action=delete_deductions. 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-2024-8567**		
Vendor: pega					
Product: infinity					
Affected Version(s): From (including) 8.1 Up to (excluding) 24.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Sep-2024	4.8	Pega Platform versions 8.1 to Infinity 24.1.2 are affected by an XSS issue with App name. **CVE ID: CVE-2024-6700**	N/A	A-PEG-INFI-180924/366
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Sep-2024	4.8	Pega Platform versions 8.1 to Infinity 24.1.2 are affected by an XSS issue with case type. **CVE ID: CVE-2024-6701**	N/A	A-PEG-INFI-180924/367
Improper Neutralization of Input During Web Page Generation	12-Sep-2024	4.8	Pega Platform versions 8.1 to Infinity 24.1.2 are affected by an HTML Injection issue with Stage.	N/A	A-PEG-INFI-180924/368

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
('Cross-site Scripting')			**CVE ID: CVE-2024-6702**		
Vendor: perfexcrm					
Product: perfex_crm					
Affected Version(s): 1.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Sep-2024	5.4	A stored cross-site scripting (XSS) vulnerability in the Discussion section of Perfex CRM v1.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Content parameter. **CVE ID: CVE-2024-44851**	N/A	A-PER-PERF-180924/369
Vendor: phpgurukul					
Product: job_portal					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	05-Sep-2024	8.8	File upload restriction bypass vulnerability in PHPGurukul Job Portal 1.0, the exploitation of which could allow an authenticated user to execute an RCE via webshell. **CVE ID: CVE-2024-8463**	N/A	A-PHP-JOB_-180924/370
Improper Neutralization of Special Elements	05-Sep-2024	7.5	SQL injection vulnerability, by which an attacker could send a specially designed	N/A	A-PHP-JOB_-180924/371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			query through JOBREGID parameter in /jobportal/admin/applicants/controller.php, and retrieve all the information stored in it. **CVE ID: CVE-2024-8464**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Sep-2024	7.5	SQL injection vulnerability, by which an attacker could send a specially designed query through user_id parameter in /jobportal/admin/user/controller.php, and retrieve all the information stored in it. **CVE ID: CVE-2024-8465**	N/A	A-PHP-JOB_-180924/372
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Sep-2024	7.5	SQL injection vulnerability, by which an attacker could send a specially designed query through CATEGORY parameter in /jobportal/admin/category/controller.php, and retrieve all the information stored in it. **CVE ID: CVE-2024-8466**	N/A	A-PHP-JOB_-180924/373
Improper Neutralizat	05-Sep-2024	7.5	SQL injection vulnerability, by	N/A	A-PHP-JOB_-180924/374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			which an attacker could send a specially designed query through id parameter in /jobportal/admin/category/index.php, and retrieve all the information stored in it. **CVE ID: CVE-2024-8467**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Sep-2024	7.5	SQL injection vulnerability, by which an attacker could send a specially designed query through search parameter in /jobportal/index.php, and retrieve all the information stored in it. **CVE ID: CVE-2024-8468**	N/A	A-PHP-JOB_-180924/375
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Sep-2024	7.5	SQL injection vulnerability, by which an attacker could send a specially designed query through id parameter in /jobportal/admin/employee/index.php, and retrieve all the information stored in it. **CVE ID: CVE-2024-8469**	N/A	A-PHP-JOB_-180924/376
Improper Neutralizat	05-Sep-2024	7.5	SQL injection vulnerability, by	N/A	A-PHP-JOB_-180924/377

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
ion of Special Elements used in an SQL Command ('SQL Injection')			which an attacker could send a specially designed query through CATEGORY parameter in /jobportal/admin/vacancy/controller.php, and retrieve all the information stored in it. **CVE ID: CVE-2024-8470**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Sep-2024	6.1	Cross-Site Scripting (XSS) vulnerability, whereby user-controlled input is not sufficiently encrypted. Exploitation of this vulnerability could allow an attacker to retrieve the session details of an authenticated user through JOBID and USERNAME parameters in /jobportal/process.php. **CVE ID: CVE-2024-8471**	N/A	A-PHP-JOB_-180924/378
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Sep-2024	6.1	Cross-Site Scripting (XSS) vulnerability, whereby user-controlled input is not sufficiently encrypted. Exploitation of this vulnerability could allow an attacker to retrieve the session details of an	N/A	A-PHP-JOB_-180924/379

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
			authenticated user through multiple parameters in /jobportal/index.php. **CVE ID: CVE-2024-8472**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Sep-2024	6.1	Cross-Site Scripting (XSS) vulnerability, whereby user-controlled input is not sufficiently encrypted. Exploitation of this vulnerability could allow an attacker to retrieve the session details of an authenticated user through user_email parameter in /jobportal/admin/login.php. **CVE ID: CVE-2024-8473**	N/A	A-PHP-JOB_-180924/380
Vendor: plechevandrey					
Product: wp-recall					
Affected Version(s): * Up to (excluding) 16.26.9					
Authorization Bypass Through User-Controlled Key	06-Sep-2024	9.8	The WP-Recall – Registration, Profile, Commerce & More plugin for WordPress is vulnerable to privilege escalation/account takeover in all versions up to, and including, 16.26.8. This is due to to plugin not properly verifying a user's	https://plugins.trac.wordpress.org/changeset/3145798/wp-recall/trunk/add-on/commerce/classes/class-rcl-create-order.php	A-PLE-WP-R-180924/381

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
			identity during new order creation. This makes it possible for unauthenticated attackers to supply any email through the user_email field and update the password for that user during new order creation. This requires the commerce addon to be enabled in order to exploit. **CVE ID: CVE-2024-8292**		
Vendor: Progress					
Product: openedge					
Affected Version(s): * Up to (including) 11.7.18					
Improper Control of Generation of Code ('Code Injection')	03-Sep-2024	9.6	Local ABL Client bypass of the required PASOE security checks may allow an attacker to commit unauthorized code injection into Multi-Session Agents on supported OpenEdge LTS platforms up to OpenEdge LTS 11.7.18 and LTS 12.2.13 on all supported release platforms **CVE ID: CVE-2024-7345**	https://community.progress.com/s/article/Direct-local-client-connections-to-MS-Agents-can-bypass-authentication	A-PRO-OPEN-180924/382
Affected Version(s): * Up to (including) 11.7.19					

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 Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	6.1	An ActiveMQ Discovery service was reachable by default from an OpenEdge Management installation when an OEE/OEM auto-discovery feature was activated. Unauthorized access to the discovery service's UDP port allowed content injection into parts of the OEM web interface making it possible for other types of attack that could spoof or deceive web interface users. Unauthorized use of the OEE/OEM discovery service was remediated by deactivating the discovery service by default. **CVE ID: CVE-2024-7654**	https://community.progress.com/s/article/Unauthenticated-Content-Injection-in-OpenEdge-Management-web-interface-via-ActiveMQ-discovery-service	A-PRO-OPEN-180924/383
Improper Authentication	03-Sep-2024	4.8	Host name validation for TLS certificates is bypassed when the installed OpenEdge default certificates are used to perform the TLS handshake for a networked connection. This has been corrected	https://community.progress.com/s/article/Client-connections-using-default-TLS-certificates-from-OpenEdge-may-bypass-TLS-	A-PRO-OPEN-180924/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			so that default certificates are no longer capable of overriding host name validation and will need to be replaced where full TLS certificate validation is needed for network security. The existing certificates should be replaced with CA-signed certificates from a recognized certificate authority that contain the necessary information to support host name validation. **CVE ID: CVE-2024-7346**	host-name-validation	
Affected Version(s): From (including) 12.0 Up to (including) 12.2.13					
Improper Control of Generation of Code ('Code Injection')	03-Sep-2024	9.6	Local ABL Client bypass of the required PASOE security checks may allow an attacker to commit unauthorized code injection into Multi-Session Agents on supported OpenEdge LTS platforms up to OpenEdge LTS 11.7.18 and LTS 12.2.13 on all supported release platforms	https://community.progress.com/s/article/Direct-local-client-connections-to-MS-Agents-can-bypass-authentication	A-PRO-OPEN-180924/385

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
			CVE ID: CVE-2024-7345		
Affected Version(s): From (including) 12.0 Up to (including) 12.2.14					
Improper Authentication	03-Sep-2024	4.8	Host name validation for TLS certificates is bypassed when the installed OpenEdge default certificates are used to perform the TLS handshake for a networked connection. This has been corrected so that default certificates are no longer capable of overriding host name validation and will need to be replaced where full TLS certificate validation is needed for network security. The existing certificates should be replaced with CA-signed certificates from a recognized certificate authority that contain the necessary information to support host name validation. **CVE ID: CVE-2024-7346**	https://community.progress.com/s/article/Client-connections-using-default-TLS-certificates-from-OpenEdge-may-bypass-TLS-host-name-validation	A-PRO-OPEN-180924/386
Affected Version(s): From (including) 12.2 Up to (including) 12.2.14					
Improper Neutralizat	03-Sep-2024	6.1	An ActiveMQ Discovery service	https://community.progress.co	A-PRO-OPEN-180924/387

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
ion of Input During Web Page Generation ('Cross-site Scripting')			was reachable by default from an OpenEdge Management installation when an OEE/OEM auto-discovery feature was activated. Unauthorized access to the discovery service's UDP port allowed content injection into parts of the OEM web interface making it possible for other types of attack that could spoof or deceive web interface users. Unauthorized use of the OEE/OEM discovery service was remediated by deactivating the discovery service by default. **CVE ID: CVE-2024-7654**	m/s/article/Unauthenticated-Content-Injection-in-OpenEdge-Management-web-interface-via-ActiveMQ-discovery-service	
Affected Version(s): From (including) 12.8 Up to (excluding) 12.8.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	6.1	An ActiveMQ Discovery service was reachable by default from an OpenEdge Management installation when an OEE/OEM auto-discovery feature was activated. Unauthorized access to the	https://community.progress.com/s/article/Unauthenticated-Content-Injection-in-OpenEdge-Management-web-interface-via-ActiveMQ-discovery-service	A-PRO-OPEN-180924/388

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
			discovery service's UDP port allowed content injection into parts of the OEM web interface making it possible for other types of attack that could spoof or deceive web interface users. Unauthorized use of the OEE/OEM discovery service was remediated by deactivating the discovery service by default. **CVE ID: CVE-2024-7654**		
Vendor: project_team					
Product: tmall_demo					
Affected Version(s): * Up to (excluding) 2024-09-01					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Sep-2024	9.8	A vulnerability, which was classified as critical, was found in Mini-Tmall up to 20240901. Affected is the function rewardMapper.select of the file tmall/admin/order/1/1. The manipulation of the argument orderBy leads to sql injection. It is possible to launch the attack remotely. The exploit has been	N/A	A-PRO-TMAL-180924/389

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
			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-2024-8568**		
Vendor: Python					
Product: python					
Affected Version(s): * Up to (including) 3.12.5					
N/A	03-Sep-2024	7.5	There is a MEDIUM severity vulnerability affecting CPython. Regular expressions that allowed excessive backtracking during tarfile.TarFile header parsing are vulnerable to ReDoS via specifically-crafted tar archives. **CVE ID: CVE-2024-6232**	https://github.com/python/cpython/commit/4eaf4891c12589e3c7bdad5f5b076e4c8392dd06, https://github.com/python/cpython/commit/743acbe872485dc18df4d8ab2dc7895187f062c4, https://github.com/python/cpython/commit/d449caf8a179e3b954268b3a88eb9170be3c8fbf	A-PYT-PYTH-180924/390
Affected Version(s): 3.13.0					
N/A	03-Sep-2024	7.5	There is a MEDIUM severity	https://github.com/python/cpython/commit/4	A-PYT-PYTH-180924/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affecting CPython. Regular expressions that allowed excessive backtracking during tarfile.TarFile header parsing are vulnerable to ReDoS via specifically-crafted tar archives. **CVE ID: CVE-2024-6232**	eaf4891c12589e3c7bdad5f5b076e4c8392dd06, https://github.com/python/cpython/commit/743acbe872485dc18df4d8ab2dc7895187f062c4, https://github.com/python/cpython/commit/d449caf8a179e3b954268b3a88eb9170be3c8fbf	
Vendor: Qnap					
Product: download_station					
Affected Version(s): From (including) 5.8.0 Up to (excluding) 5.8.6.283					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect Download Station. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following version:	https://www.qnap.com/en/security-advisory/qsa-24-35	A-QNA-DOWN-180924/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Download Station 5.8.6.283 (2024/06/21) and later **CVE ID: CVE-2024-38640**		
Product: helpdesk					
Affected Version(s): * Up to (excluding) 3.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect Helpdesk. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following version: Helpdesk 3.3.1 and later **CVE ID: CVE-2024-27125**	https://www.qnap.com/en/security-advisory/qsa-24-29	A-QNA-HELP-180924/393
Product: notes_station_3					
Affected Version(s): * Up to (excluding) 3.9.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect Notes Station 3. If exploited, the vulnerability could allow authenticated users	https://www.qnap.com/en/security-advisory/qsa-24-21	A-QNA-NOTE-180924/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to inject malicious code via a network. We have already fixed the vulnerability in the following versions: Notes Station 3 3.9.6 and later **CVE ID: CVE-2024-27126**		
Affected Version(s): From (including) 3.3.9.0 Up to (excluding) 3.3.9.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect Notes Station 3. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions: Notes Station 3 3.9.6 and later **CVE ID: CVE-2024-27122**	https://www.qnap.com/en/security-advisory/qsa-24-21	A-QNA-NOTE-180924/395
Product: qulog_center					
Affected Version(s): From (including) 1.7.0 Up to (excluding) 1.7.0.827					
Improper Neutralization of Input During Web Page Generation	06-Sep-2024	6.1	A cross-site scripting (XSS) vulnerability has been reported to affect QuLog Center. If exploited,	https://www.qnap.com/en/security-advisory/qsa-24-30	A-QNA-QULO-180924/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			the vulnerability could allow users to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QuLog Center 1.8.0.872 (2024/06/17) and later QuLog Center 1.7.0.827 (2024/06/17) and later **CVE ID: CVE-2024-32762**		
Affected Version(s): From (including) 1.8.0 Up to (excluding) 1.8.0.872					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	6.1	A cross-site scripting (XSS) vulnerability has been reported to affect QuLog Center. If exploited, the vulnerability could allow users to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QuLog Center 1.8.0.872 (2024/06/17) and later	https://www.qnap.com/en/security-advisory/qsa-24-30	A-QNA-QULO-180924/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QuLog Center 1.7.0.827 (2024/06/17) and later **CVE ID: CVE-2024-32762**		
Product: qumagie					
Affected Version(s): 2.3.0					
Improper Certificate Validation	06-Sep-2024	7.8	An improper certificate validation vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow local network users to compromise the security of the system via unspecified vectors. We have already fixed the vulnerability in the following version: QuMagie 2.3.1 and later **CVE ID: CVE-2024-38642**	https://www.qnap.com/en/security-advisory/qsa-24-34	A-QNA-QUMA-180924/398
Vendor: raspcontrol_project					
Product: raspcontrol					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page	04-Sep-2024	6.1	Cross Site Scripting (XSS) vulnerability through the action parameter in index.php. Affected	N/A	A-RAS-RASP-180924/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			product codebase https://github.com/Bioshox/Raspcontrol and forks such as https://github.com/harmon25/raspcontrol . An attacker could exploit this vulnerability by sending a specially crafted JavaScript payload to an authenticated user and partially hijacking their session details. References list **CVE ID: CVE-2024-8413**		
Vendor: rdkcentral					
Product: rdk-b					
Affected Version(s): 2022q3					
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558; Issue ID: MSV-1526.	https://corp.mediatek.com/product-security-bulletin/September-2024	A-RDK-RDK--180924/400

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
			CVE ID: CVE-2024-20089		
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	A-RDK-RDK--180924/401
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	A-RDK-RDK--180924/402
Vendor: rdstation					
Product: rd_station					
Affected Version(s): * Up to (excluding) 5.4.0					

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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Sep-2024	5.4	The RD Station plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 5.3.2 due to insufficient input sanitization and output escaping of post metaboxes added by the plugin. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-6894**	N/A	A-RDS-RD_S-180924/403
Vendor: Redhat					
Product: build_of_keycloak					
Affected Version(s): From (including) 22.0 Up to (excluding) 22.012					
Improper Enforcement of a Single, Unique Action	03-Sep-2024	6.5	A vulnerability was found in Keycloak. This flaw allows attackers to bypass brute force protection by exploiting the timing of login attempts. By initiating multiple login requests simultaneously,	https://access.redhat.com/errata/RHSA-2024:6493, https://access.redhat.com/errata/RHSA-2024:6494, https://access.redhat.com/errata/RHSA-2024:6495,	A-RED-BUIL-180924/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers can exceed the configured limits for failed attempts before the system locks them out. This timing loophole enables attackers to make more guesses at passwords than intended, potentially compromising account security on affected systems. **CVE ID: CVE-2024-4629**	https://access.redhat.com/errata/RHSA-2024:6497, https://access.redhat.com/errata/RHSA-2024:6499	
Product: keycloak					
Affected Version(s): * Up to (excluding) 24.0.3					
Improper Enforcement of a Single, Unique Action	03-Sep-2024	6.5	A vulnerability was found in Keycloak. This flaw allows attackers to bypass brute force protection by exploiting the timing of login attempts. By initiating multiple login requests simultaneously, attackers can exceed the configured limits for failed attempts before the system locks them out. This timing loophole enables attackers to make more guesses at passwords than	https://access.redhat.com/errata/RHSA-2024:6493, https://access.redhat.com/errata/RHSA-2024:6494, https://access.redhat.com/errata/RHSA-2024:6495, https://access.redhat.com/errata/RHSA-2024:6497, https://access.redhat.com/errata/RHSA-2024:6499	A-RED-KEYC-180924/405

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
			intended, potentially compromising account security on affected systems. **CVE ID: CVE-2024-4629**		
Product: openshift_container_platform					
Affected Version(s): 4.11					
Improper Enforcement of a Single, Unique Action	03-Sep-2024	6.5	A vulnerability was found in Keycloak. This flaw allows attackers to bypass brute force protection by exploiting the timing of login attempts. By initiating multiple login requests simultaneously, attackers can exceed the configured limits for failed attempts before the system locks them out. This timing loophole enables attackers to make more guesses at passwords than intended, potentially compromising account security on affected systems. **CVE ID: CVE-2024-4629**	https://access.redhat.com/errata/RHSA-2024:6493, https://access.redhat.com/errata/RHSA-2024:6494, https://access.redhat.com/errata/RHSA-2024:6495, https://access.redhat.com/errata/RHSA-2024:6497, https://access.redhat.com/errata/RHSA-2024:6499	A-RED-OPEN-180924/406
Affected Version(s): 4.12					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Enforcement of a Single, Unique Action	03-Sep-2024	6.5	A vulnerability was found in Keycloak. This flaw allows attackers to bypass brute force protection by exploiting the timing of login attempts. By initiating multiple login requests simultaneously, attackers can exceed the configured limits for failed attempts before the system locks them out. This timing loophole enables attackers to make more guesses at passwords than intended, potentially compromising account security on affected systems. **CVE ID: CVE-2024-4629**	https://access.redhat.com/errata/RHSA-2024:6493, https://access.redhat.com/errata/RHSA-2024:6494, https://access.redhat.com/errata/RHSA-2024:6495, https://access.redhat.com/errata/RHSA-2024:6497, https://access.redhat.com/errata/RHSA-2024:6499	A-RED-OPEN-180924/407
Product: openshift_container_platform_for_linuxone					
Affected Version(s): 4.10					
Improper Enforcement of a Single, Unique Action	03-Sep-2024	6.5	A vulnerability was found in Keycloak. This flaw allows attackers to bypass brute force protection by exploiting the timing of login attempts. By initiating multiple login requests	https://access.redhat.com/errata/RHSA-2024:6493, https://access.redhat.com/errata/RHSA-2024:6494, https://access.redhat.com/errata/RHSA-	A-RED-OPEN-180924/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			simultaneously, attackers can exceed the configured limits for failed attempts before the system locks them out. This timing loophole enables attackers to make more guesses at passwords than intended, potentially compromising account security on affected systems. **CVE ID: CVE-2024-4629**	2024:6495, https://access.redhat.com/errata/RHSA-2024:6497, https://access.redhat.com/errata/RHSA-2024:6499	
Affected Version(s): 4.9					
Improper Enforcement of a Single, Unique Action	03-Sep-2024	6.5	A vulnerability was found in Keycloak. This flaw allows attackers to bypass brute force protection by exploiting the timing of login attempts. By initiating multiple login requests simultaneously, attackers can exceed the configured limits for failed attempts before the system locks them out. This timing loophole enables attackers to make more guesses at passwords than	https://access.redhat.com/errata/RHSA-2024:6493, https://access.redhat.com/errata/RHSA-2024:6494, https://access.redhat.com/errata/RHSA-2024:6495, https://access.redhat.com/errata/RHSA-2024:6497, https://access.redhat.com/errata/RHSA-2024:6499	A-RED-OPEN-180924/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intended, potentially compromising account security on affected systems. **CVE ID: CVE-2024-4629**		
Product: openshift_container_platform_for_power					
Affected Version(s): 4.10					
Improper Enforcement of a Single, Unique Action	03-Sep-2024	6.5	A vulnerability was found in Keycloak. This flaw allows attackers to bypass brute force protection by exploiting the timing of login attempts. By initiating multiple login requests simultaneously, attackers can exceed the configured limits for failed attempts before the system locks them out. This timing loophole enables attackers to make more guesses at passwords than intended, potentially compromising account security on affected systems. **CVE ID: CVE-2024-4629**	https://access.redhat.com/errata/RHSA-2024:6493, https://access.redhat.com/errata/RHSA-2024:6494, https://access.redhat.com/errata/RHSA-2024:6495, https://access.redhat.com/errata/RHSA-2024:6497, https://access.redhat.com/errata/RHSA-2024:6499	A-RED-OPEN-180924/410
Affected Version(s): 4.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Enforcement of a Single, Unique Action	03-Sep-2024	6.5	A vulnerability was found in Keycloak. This flaw allows attackers to bypass brute force protection by exploiting the timing of login attempts. By initiating multiple login requests simultaneously, attackers can exceed the configured limits for failed attempts before the system locks them out. This timing loophole enables attackers to make more guesses at passwords than intended, potentially compromising account security on affected systems. **CVE ID: CVE-2024-4629**	https://access.redhat.com/errata/RHSA-2024:6493, https://access.redhat.com/errata/RHSA-2024:6494, https://access.redhat.com/errata/RHSA-2024:6495, https://access.redhat.com/errata/RHSA-2024:6497, https://access.redhat.com/errata/RHSA-2024:6499	A-RED-OPEN-180924/411
Product: openshift_container_platform_ibm_z_systems					
Affected Version(s): 4.10					
Improper Enforcement of a Single, Unique Action	03-Sep-2024	6.5	A vulnerability was found in Keycloak. This flaw allows attackers to bypass brute force protection by exploiting the timing of login attempts. By initiating multiple login requests	https://access.redhat.com/errata/RHSA-2024:6493, https://access.redhat.com/errata/RHSA-2024:6494, https://access.redhat.com/errata/RHSA-	A-RED-OPEN-180924/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			simultaneously, attackers can exceed the configured limits for failed attempts before the system locks them out. This timing loophole enables attackers to make more guesses at passwords than intended, potentially compromising account security on affected systems. **CVE ID: CVE-2024-4629**	2024:6495, https://access.redhat.com/errata/RHSA-2024:6497, https://access.redhat.com/errata/RHSA-2024:6499	
Affected Version(s): 4.9					
Improper Enforcement of a Single, Unique Action	03-Sep-2024	6.5	A vulnerability was found in Keycloak. This flaw allows attackers to bypass brute force protection by exploiting the timing of login attempts. By initiating multiple login requests simultaneously, attackers can exceed the configured limits for failed attempts before the system locks them out. This timing loophole enables attackers to make more guesses at passwords than	https://access.redhat.com/errata/RHSA-2024:6493, https://access.redhat.com/errata/RHSA-2024:6494, https://access.redhat.com/errata/RHSA-2024:6495, https://access.redhat.com/errata/RHSA-2024:6497, https://access.redhat.com/errata/RHSA-2024:6499	A-RED-OPEN-180924/413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intended, potentially compromising account security on affected systems. **CVE ID: CVE-2024-4629**		
Product: satellite					
Affected Version(s): 6.13					
Improper Authentication	04-Sep-2024	9.8	An authentication bypass vulnerability has been identified in Foreman when deployed with External Authentication, due to the puppet-foreman configuration. This issue arises from Apache's mod_proxy not properly unsetting headers because of restrictions on underscores in HTTP headers, allowing authentication through a malformed header. This flaw impacts all active Satellite deployments (6.13, 6.14 and 6.15) and could potentially enable unauthorized users to gain administrative access.	https://access.redhat.com/errata/RHSA-2024:6335, https://access.redhat.com/errata/RHSA-2024:6336, https://access.redhat.com/errata/RHSA-2024:6337, https://access.redhat.com/security/cve/CVE-2024-7012	A-RED-SATE-180924/414

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
			CVE ID: CVE-2024-7012		
Improper Authentication	04-Sep-2024	9.8	An authentication bypass vulnerability has been identified in Pulpcore when deployed with Gunicorn versions prior to 22.0, due to the puppet-pulpcore configuration. This issue arises from Apache's mod_proxy not properly unsetting headers because of restrictions on underscores in HTTP headers, allowing authentication through a malformed header. This flaw impacts all active Satellite deployments (6.13, 6.14 and 6.15) which are using Pulpcore version 3.0+ and could potentially enable unauthorized users to gain administrative access. **CVE ID: CVE-2024-7923**	https://access.redhat.com/errata/RHSA-2024:6335, https://access.redhat.com/errata/RHSA-2024:6336, https://access.redhat.com/errata/RHSA-2024:6337, https://access.redhat.com/security/cve/CVE-2024-7923	A-RED-SATE-180924/415
Affected Version(s): 6.14					

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 Authentication	04-Sep-2024	9.8	An authentication bypass vulnerability has been identified in Foreman when deployed with External Authentication, due to the puppet-foreman configuration. This issue arises from Apache's mod_proxy not properly unsetting headers because of restrictions on underscores in HTTP headers, allowing authentication through a malformed header. This flaw impacts all active Satellite deployments (6.13, 6.14 and 6.15) and could potentially enable unauthorized users to gain administrative access. **CVE ID: CVE-2024-7012**	https://access.redhat.com/errata/RHSA-2024:6335, https://access.redhat.com/errata/RHSA-2024:6336, https://access.redhat.com/errata/RHSA-2024:6337, https://access.redhat.com/security/cve/CVE-2024-7012	A-RED-SATE-180924/416
Improper Authentication	04-Sep-2024	9.8	An authentication bypass vulnerability has been identified in Pulpcore when deployed with Gunicorn versions prior to 22.0, due to	https://access.redhat.com/errata/RHSA-2024:6335, https://access.redhat.com/errata/RHSA-2024:6336,	A-RED-SATE-180924/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the puppet-pulpcore configuration. This issue arises from Apache's mod_proxy not properly unsetting headers because of restrictions on underscores in HTTP headers, allowing authentication through a malformed header. This flaw impacts all active Satellite deployments (6.13, 6.14 and 6.15) which are using Pulpcore version 3.0+ and could potentially enable unauthorized users to gain administrative access. **CVE ID: CVE-2024-7923**	https://access.redhat.com/errata/RHSA-2024:6337, https://access.redhat.com/security/cve/CVE-2024-7923	
Affected Version(s): 6.15					
Improper Authentication	04-Sep-2024	9.8	An authentication bypass vulnerability has been identified in Foreman when deployed with External Authentication, due to the puppet-foreman configuration. This issue arises from Apache's	https://access.redhat.com/errata/RHSA-2024:6335, https://access.redhat.com/errata/RHSA-2024:6336, https://access.redhat.com/errata/RHSA-2024:6337, https://access.r	A-RED-SATE-180924/418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mod_proxy not properly unsetting headers because of restrictions on underscores in HTTP headers, allowing authentication through a malformed header. This flaw impacts all active Satellite deployments (6.13, 6.14 and 6.15) and could potentially enable unauthorized users to gain administrative access. **CVE ID: CVE-2024-7012**	edhat.com/security/cve/CVE-2024-7012	
Improper Authentication	04-Sep-2024	9.8	An authentication bypass vulnerability has been identified in Pulpcore when deployed with Gunicorn versions prior to 22.0, due to the puppet-pulpcore configuration. This issue arises from Apache's mod_proxy not properly unsetting headers because of restrictions on underscores in HTTP headers, allowing authentication	https://access.redhat.com/errata/RHSA-2024:6335, https://access.redhat.com/errata/RHSA-2024:6336, https://access.redhat.com/errata/RHSA-2024:6337, https://access.redhat.com/security/cve/CVE-2024-7923	A-RED-SATE-180924/419

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
			through a malformed header. This flaw impacts all active Satellite deployments (6.13, 6.14 and 6.15) which are using Pulpcore version 3.0+ and could potentially enable unauthorized users to gain administrative access. **CVE ID: CVE-2024-7923**		
Product: single_sign-on					
Affected Version(s): -					
Improper Enforcement of a Single, Unique Action	03-Sep-2024	6.5	A vulnerability was found in Keycloak. This flaw allows attackers to bypass brute force protection by exploiting the timing of login attempts. By initiating multiple login requests simultaneously, attackers can exceed the configured limits for failed attempts before the system locks them out. This timing loophole enables attackers to make more guesses at passwords than intended, potentially	https://access.redhat.com/errata/RHSA-2024:6493, https://access.redhat.com/errata/RHSA-2024:6494, https://access.redhat.com/errata/RHSA-2024:6495, https://access.redhat.com/errata/RHSA-2024:6497, https://access.redhat.com/errata/RHSA-2024:6499	A-RED-SING-180924/420

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
			compromising account security on affected systems. **CVE ID: CVE-2024-4629**		
Affected Version(s): From (including) 7.6 Up to (excluding) 7.6.10					
Improper Enforcement of a Single, Unique Action	03-Sep-2024	6.5	A vulnerability was found in Keycloak. This flaw allows attackers to bypass brute force protection by exploiting the timing of login attempts. By initiating multiple login requests simultaneously, attackers can exceed the configured limits for failed attempts before the system locks them out. This timing loophole enables attackers to make more guesses at passwords than intended, potentially compromising account security on affected systems. **CVE ID: CVE-2024-4629**	https://access.redhat.com/errata/RHSA-2024:6493, https://access.redhat.com/errata/RHSA-2024:6494, https://access.redhat.com/errata/RHSA-2024:6495, https://access.redhat.com/errata/RHSA-2024:6497, https://access.redhat.com/errata/RHSA-2024:6499	A-RED-SING-180924/421
Vendor: rems					
Product: contact_manager_with_export_to_vcf					
Affected Version(s): 1.0					
Improper Neutralizat	03-Sep-2024	9.8	A vulnerability was found in	N/A	A-REM-CONT-180924/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			SourceCodester Contact Manager with Export to VCF 1.0. It has been rated as critical. This issue affects some unknown processing of the file /endpoint/delete-account.php of the component Delete Contact Handler. The manipulation of the argument contact 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-2024-8380**		
Product: php_crud					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Sep-2024	9.8	A vulnerability has been found in SourceCodester PHP CRUD 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /endpoint/delete.php of the component Delete Person Handler. The manipulation of the argument	N/A	A-REM-PHP_-180924/423

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
			person leads to sql injection. The attack can be launched remotely. **CVE ID: CVE-2024-8561**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Sep-2024	8.8	A vulnerability was found in SourceCodester PHP CRUD 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /endpoint/update.php. The manipulation of the argument tbl_person_id/first_name/middle_name/last_name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8564**	N/A	A-REM-PHP_-180924/424
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-2024	6.1	A vulnerability was found in SourceCodester PHP CRUD 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /endpoint/Add.ph	N/A	A-REM-PHP_-180924/425

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
			p. The manipulation of the argument first_name/middle_name/last_name 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-2024-8562**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-2024	6.1	A vulnerability was found in SourceCodester PHP CRUD 1.0. It has been classified as problematic. This affects an unknown part of the file /endpoint/update.php. The manipulation of the argument first_name/middle_name/last_name 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. **CVE ID: CVE-2024-8563**	https://vuldb.com/?id.276783	A-REM-PHP_-180924/426
Vendor: remyandrade					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: online_food_menu					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Sep-2024	7.2	A vulnerability, which was classified as critical, has been found in SourceCodester Online Food Menu 1.0. This issue affects some unknown processing of the file /endpoint/delete-menu.php. The manipulation of the argument menu 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-2024-8559**	N/A	A-REM-ONLI-180924/427
Vendor: rocket.chat					
Product: rocket.chat					
Affected Version(s): * Up to (including) 6.3.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-2024	5.4	The Electron desktop application of Rocket.Chat through 6.3.4 allows stored XSS via links in an uploaded file, related to failure to use a separate browser upon encountering third-party external	N/A	A-ROC-ROCK-180924/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			actions from PDF documents. **CVE ID: CVE-2024-45621**		
Vendor: salesagility					
Product: suitecrm					
Affected Version(s): * Up to (excluding) 7.14.5					
N/A	05-Sep-2024	4.3	SuiteCRM is an open-source customer relationship management (CRM) system. Prior to version 7.14.5 and 8.6.2, insufficient access control checks allow a threat actor to delete records via the API. Versions 7.14.5 and 8.6.2 contain a patch for the issue. **CVE ID: CVE-2024-45392**	N/A	A-SAL-SUIT-180924/429
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.6.2					
N/A	05-Sep-2024	4.3	SuiteCRM is an open-source customer relationship management (CRM) system. Prior to version 7.14.5 and 8.6.2, insufficient access control checks allow a threat actor to delete records via the API. Versions 7.14.5 and	N/A	A-SAL-SUIT-180924/430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.6.2 contain a patch for the issue. **CVE ID: CVE-2024-45392**		
Vendor: sambas					
Product: akos					
Affected Version(s): * Up to (including) 2024-09-02					
N/A	03-Sep-2024	9.8	Improper Privilege Management vulnerability in SAMPA? Holding AKOS allows Collect Data as Provided by Users.This issue affects AKOS: through 20240902. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-4259**	N/A	A-SAM-AKOS-180924/431
Vendor: Samsung					
Product: assistant					
Affected Version(s): * Up to (excluding) 9.1.00.7					
Incorrect Default Permissions	04-Sep-2024	4.3	Improper handling of insufficient permissions in Samsung Assistant prior to version 9.1.00.7 allows remote attackers to access location data. User interaction is	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=09	A-SAM-ASSI-180924/432

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
			required for triggering this vulnerability. **CVE ID: CVE-2024-34661**		
Product: group_sharing					
Affected Version(s): * Up to (excluding) 13.6.13.3					
N/A	04-Sep-2024	5.3	Exposure of sensitive information in GroupSharing prior to version 13.6.13.3 allows remote attackers can force the victim to join the group. **CVE ID: CVE-2024-34659**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=09	A-SAM-GROU-180924/433
Product: notes					
Affected Version(s): * Up to (excluding) 4.4.21.62					
Out-of-bounds Write	04-Sep-2024	9.8	Stack-based out-of-bounds write in Samsung Notes prior to version 4.4.21.62 allows remote attackers to execute arbitrary code. **CVE ID: CVE-2024-34657**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=09	A-SAM-NOTE-180924/434
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Sep-2024	7.8	Path traversal in Samsung Notes prior to version 4.4.21.62 allows local attackers to execute arbitrary code. **CVE ID: CVE-2024-34656**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=09	A-SAM-NOTE-180924/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Sep-2024	7.8	Heap-based out-of-bounds write in Samsung Notes prior to version 4.4.21.62 allows local attackers to execute arbitrary code. **CVE ID: CVE-2024-34660**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=09	A-SAM-NOTE-180924/436
Out-of-bounds Read	04-Sep-2024	7.1	Out-of-bounds read in Samsung Notes allows local attackers to bypass ASLR. **CVE ID: CVE-2024-34658**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=09	A-SAM-NOTE-180924/437
Product: universal_print_driver					
Affected Version(s): 3.00.16.0101					
N/A	11-Sep-2024	7.8	The Samsung Universal Print Driver for Windows is potentially vulnerable to escalation of privilege allowing the creation of a reverse shell in the tool. This is only applicable for products in the application released or manufactured before 2018. **CVE ID: CVE-2024-5760**	N/A	A-SAM-UNIV-180924/438
Vendor: SAP					
Product: netweaver_application_server_abap					
Affected Version(s): 700					

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
Missing Authorization	10-Sep-2024	2.7	Due to missing authorization check, SAP NetWeaver Application Server for ABAP and ABAP Platform allows an attacker logged in as a developer to read objects contained in a package. This causes an impact on confidentiality, as this attacker would otherwise not have access to view these objects. **CVE ID: CVE-2024-41728**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/439
Affected Version(s): 701					
Missing Authorization	10-Sep-2024	2.7	Due to missing authorization check, SAP NetWeaver Application Server for ABAP and ABAP Platform allows an attacker logged in as a developer to read objects contained in a package. This causes an impact on confidentiality, as this attacker would otherwise not have access to view these objects. **CVE ID: CVE-2024-41728**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/440
Affected Version(s): 702					

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
Incorrect Authorization	10-Sep-2024	2.7	SAP NetWeaver Application Server for ABAP and ABAP Platform allow users with high privileges to execute a program that reveals data over the network. This results in a minimal impact on confidentiality of the application. **CVE ID: CVE-2024-44114**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/441
Missing Authorization	10-Sep-2024	2.7	Due to missing authorization check, SAP NetWeaver Application Server for ABAP and ABAP Platform allows an attacker logged in as a developer to read objects contained in a package. This causes an impact on confidentiality, as this attacker would otherwise not have access to view these objects. **CVE ID: CVE-2024-41728**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/442
Affected Version(s): 731					
Incorrect Authorization	10-Sep-2024	2.7	SAP NetWeaver Application Server for ABAP and ABAP Platform allow users with high privileges to	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/443

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
			execute a program that reveals data over the network. This results in a minimal impact on confidentiality of the application. **CVE ID: CVE-2024-44114**		
Missing Authorization	10-Sep-2024	2.7	Due to missing authorization check, SAP NetWeaver Application Server for ABAP and ABAP Platform allows an attacker logged in as a developer to read objects contained in a package. This causes an impact on confidentiality, as this attacker would otherwise not have access to view these objects. **CVE ID: CVE-2024-41728**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/444
Affected Version(s): 740					
Incorrect Authorization	10-Sep-2024	2.7	SAP NetWeaver Application Server for ABAP and ABAP Platform allow users with high privileges to execute a program that reveals data over the network. This results in a minimal impact on	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/445

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
			confidentiality of the application. **CVE ID: CVE-2024-44114**		
Missing Authorization	10-Sep-2024	2.7	Due to missing authorization check, SAP NetWeaver Application Server for ABAP and ABAP Platform allows an attacker logged in as a developer to read objects contained in a package. This causes an impact on confidentiality, as this attacker would otherwise not have access to view these objects. **CVE ID: CVE-2024-41728**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/446
Affected Version(s): 750					
Incorrect Authorization	10-Sep-2024	2.7	SAP NetWeaver Application Server for ABAP and ABAP Platform allow users with high privileges to execute a program that reveals data over the network. This results in a minimal impact on confidentiality of the application. **CVE ID: CVE-2024-44114**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/447

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
Missing Authorization	10-Sep-2024	2.7	Due to missing authorization check, SAP NetWeaver Application Server for ABAP and ABAP Platform allows an attacker logged in as a developer to read objects contained in a package. This causes an impact on confidentiality, as this attacker would otherwise not have access to view these objects. **CVE ID: CVE-2024-41728**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/448
Affected Version(s): 751					
Incorrect Authorization	10-Sep-2024	2.7	SAP NetWeaver Application Server for ABAP and ABAP Platform allow users with high privileges to execute a program that reveals data over the network. This results in a minimal impact on confidentiality of the application. **CVE ID: CVE-2024-44114**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/449
Missing Authorization	10-Sep-2024	2.7	Due to missing authorization check, SAP NetWeaver Application Server for ABAP and ABAP	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/450

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
			Platform allows an attacker logged in as a developer to read objects contained in a package. This causes an impact on confidentiality, as this attacker would otherwise not have access to view these objects. **CVE ID: CVE-2024-41728**		
Affected Version(s): 752					
Incorrect Authorization	10-Sep-2024	2.7	SAP NetWeaver Application Server for ABAP and ABAP Platform allow users with high privileges to execute a program that reveals data over the network. This results in a minimal impact on confidentiality of the application. **CVE ID: CVE-2024-44114**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/451
Missing Authorization	10-Sep-2024	2.7	Due to missing authorization check, SAP NetWeaver Application Server for ABAP and ABAP Platform allows an attacker logged in as a developer to read objects contained in a package. This	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causes an impact on confidentiality, as this attacker would otherwise not have access to view these objects. **CVE ID: CVE-2024-41728**		
Affected Version(s): 753					
Incorrect Authorization	10-Sep-2024	2.7	SAP NetWeaver Application Server for ABAP and ABAP Platform allow users with high privileges to execute a program that reveals data over the network. This results in a minimal impact on confidentiality of the application. **CVE ID: CVE-2024-44114**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/453
Missing Authorization	10-Sep-2024	2.7	Due to missing authorization check, SAP NetWeaver Application Server for ABAP and ABAP Platform allows an attacker logged in as a developer to read objects contained in a package. This causes an impact on confidentiality, as this attacker would otherwise not have access to view these objects.	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/454

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
			CVE ID: CVE-2024-41728		
Affected Version(s): 754					
Incorrect Authorization	10-Sep-2024	2.7	SAP NetWeaver Application Server for ABAP and ABAP Platform allow users with high privileges to execute a program that reveals data over the network. This results in a minimal impact on confidentiality of the application. **CVE ID: CVE-2024-44114**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/455
Missing Authorization	10-Sep-2024	2.7	Due to missing authorization check, SAP NetWeaver Application Server for ABAP and ABAP Platform allows an attacker logged in as a developer to read objects contained in a package. This causes an impact on confidentiality, as this attacker would otherwise not have access to view these objects. **CVE ID: CVE-2024-41728**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/456
Affected Version(s): 755					

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
Incorrect Authorization	10-Sep-2024	2.7	SAP NetWeaver Application Server for ABAP and ABAP Platform allow users with high privileges to execute a program that reveals data over the network. This results in a minimal impact on confidentiality of the application. **CVE ID: CVE-2024-44114**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/457
Missing Authorization	10-Sep-2024	2.7	Due to missing authorization check, SAP NetWeaver Application Server for ABAP and ABAP Platform allows an attacker logged in as a developer to read objects contained in a package. This causes an impact on confidentiality, as this attacker would otherwise not have access to view these objects. **CVE ID: CVE-2024-41728**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/458
Affected Version(s): 756					
Incorrect Authorization	10-Sep-2024	2.7	SAP NetWeaver Application Server for ABAP and ABAP Platform allow users with high privileges to	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/459

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
			execute a program that reveals data over the network. This results in a minimal impact on confidentiality of the application. **CVE ID: CVE-2024-44114**		
Missing Authorization	10-Sep-2024	2.7	Due to missing authorization check, SAP NetWeaver Application Server for ABAP and ABAP Platform allows an attacker logged in as a developer to read objects contained in a package. This causes an impact on confidentiality, as this attacker would otherwise not have access to view these objects. **CVE ID: CVE-2024-41728**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/460
Affected Version(s): 757					
Incorrect Authorization	10-Sep-2024	2.7	SAP NetWeaver Application Server for ABAP and ABAP Platform allow users with high privileges to execute a program that reveals data over the network. This results in a minimal impact on	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/461

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
			confidentiality of the application. **CVE ID: CVE-2024-44114**		
Missing Authorization	10-Sep-2024	2.7	Due to missing authorization check, SAP NetWeaver Application Server for ABAP and ABAP Platform allows an attacker logged in as a developer to read objects contained in a package. This causes an impact on confidentiality, as this attacker would otherwise not have access to view these objects. **CVE ID: CVE-2024-41728**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/462
Affected Version(s): 758					
Incorrect Authorization	10-Sep-2024	2.7	SAP NetWeaver Application Server for ABAP and ABAP Platform allow users with high privileges to execute a program that reveals data over the network. This results in a minimal impact on confidentiality of the application. **CVE ID: CVE-2024-44114**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/463

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
Missing Authorization	10-Sep-2024	2.7	Due to missing authorization check, SAP NetWeaver Application Server for ABAP and ABAP Platform allows an attacker logged in as a developer to read objects contained in a package. This causes an impact on confidentiality, as this attacker would otherwise not have access to view these objects. **CVE ID: CVE-2024-41728**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/464
Affected Version(s): 912					
Incorrect Authorization	10-Sep-2024	2.7	SAP NetWeaver Application Server for ABAP and ABAP Platform allow users with high privileges to execute a program that reveals data over the network. This results in a minimal impact on confidentiality of the application. **CVE ID: CVE-2024-44114**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/465
Missing Authorization	10-Sep-2024	2.7	Due to missing authorization check, SAP NetWeaver Application Server for ABAP and ABAP	https://url.sap/sapsecuritypatchday	A-SAP-NETW-180924/466

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
			Platform allows an attacker logged in as a developer to read objects contained in a package. This causes an impact on confidentiality, as this attacker would otherwise not have access to view these objects. **CVE ID: CVE-2024-41728**		
Product: oil_\%\/_gas					
Affected Version(s): 600					
Missing Authorization	10-Sep-2024	4.3	Due to missing authorization check in SAP for Oil & Gas (Transportation and Distribution), an attacker authenticated as a non-administrative user could call a remote-enabled function which will allow them to delete non-sensitive entries in a user data table. There is no effect on confidentiality or availability. **CVE ID: CVE-2024-44112**	https://url.sap/sapsecuritypatchday	A-SAP-OIL_-180924/467
Affected Version(s): 602					
Missing Authorization	10-Sep-2024	4.3	Due to missing authorization check in SAP for Oil & Gas	https://url.sap/sapsecuritypatchday	A-SAP-OIL_-180924/468

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
			(Transportation and Distribution), an attacker authenticated as a non-administrative user could call a remote-enabled function which will allow them to delete non-sensitive entries in a user data table. There is no effect on confidentiality or availability. **CVE ID: CVE-2024-44112**		
Affected Version(s): 603					
Missing Authorization	10-Sep-2024	4.3	Due to missing authorization check in SAP for Oil & Gas (Transportation and Distribution), an attacker authenticated as a non-administrative user could call a remote-enabled function which will allow them to delete non-sensitive entries in a user data table. There is no effect on confidentiality or availability. **CVE ID: CVE-2024-44112**	https://url.sap/sapsecuritypatchday	A-SAP-OIL_-180924/469
Affected Version(s): 604					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-Sep-2024	4.3	Due to missing authorization check in SAP for Oil & Gas (Transportation and Distribution), an attacker authenticated as a non-administrative user could call a remote-enabled function which will allow them to delete non-sensitive entries in a user data table. There is no effect on confidentiality or availability. **CVE ID: CVE-2024-44112**	https://url.sap/sapsecuritypatchday	A-SAP-OIL_-180924/470
Affected Version(s): 605					
Missing Authorization	10-Sep-2024	4.3	Due to missing authorization check in SAP for Oil & Gas (Transportation and Distribution), an attacker authenticated as a non-administrative user could call a remote-enabled function which will allow them to delete non-sensitive entries in a user data table. There is no effect on confidentiality or availability.	https://url.sap/sapsecuritypatchday	A-SAP-OIL_-180924/471

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
			CVE ID: CVE-2024-44112		
Affected Version(s): 606					
Missing Authorization	10-Sep-2024	4.3	Due to missing authorization check in SAP for Oil & Gas (Transportation and Distribution), an attacker authenticated as a non-administrative user could call a remote-enabled function which will allow them to delete non-sensitive entries in a user data table. There is no effect on confidentiality or availability. **CVE ID: CVE-2024-44112**	https://url.sap/sapsecuritypatchday	A-SAP-OIL_-180924/472
Affected Version(s): 617					
Missing Authorization	10-Sep-2024	4.3	Due to missing authorization check in SAP for Oil & Gas (Transportation and Distribution), an attacker authenticated as a non-administrative user could call a remote-enabled function which will allow them to delete non-sensitive entries in a user data table. There is no effect	https://url.sap/sapsecuritypatchday	A-SAP-OIL_-180924/473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on confidentiality or availability. **CVE ID: CVE-2024-44112**		
Affected Version(s): 618					
Missing Authorization	10-Sep-2024	4.3	Due to missing authorization check in SAP for Oil & Gas (Transportation and Distribution), an attacker authenticated as a non-administrative user could call a remote-enabled function which will allow them to delete non-sensitive entries in a user data table. There is no effect on confidentiality or availability. **CVE ID: CVE-2024-44112**	https://url.sap/sapsecuritypatchday	A-SAP-OIL_-180924/474
Affected Version(s): 800					
Missing Authorization	10-Sep-2024	4.3	Due to missing authorization check in SAP for Oil & Gas (Transportation and Distribution), an attacker authenticated as a non-administrative user could call a remote-enabled function which will allow them to delete non-sensitive entries in	https://url.sap/sapsecuritypatchday	A-SAP-OIL_-180924/475

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
			a user data table. There is no effect on confidentiality or availability. **CVE ID: CVE-2024-44112**		
Affected Version(s): 802					
Missing Authorization	10-Sep-2024	4.3	Due to missing authorization check in SAP for Oil & Gas (Transportation and Distribution), an attacker authenticated as a non-administrative user could call a remote-enabled function which will allow them to delete non-sensitive entries in a user data table. There is no effect on confidentiality or availability. **CVE ID: CVE-2024-44112**	https://url.sap/sapsecuritypatchday	A-SAP-OIL_-180924/476
Affected Version(s): 803					
Missing Authorization	10-Sep-2024	4.3	Due to missing authorization check in SAP for Oil & Gas (Transportation and Distribution), an attacker authenticated as a non-administrative user could call a remote-enabled function which will allow them to	https://url.sap/sapsecuritypatchday	A-SAP-OIL_-180924/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			delete non-sensitive entries in a user data table. There is no effect on confidentiality or availability. **CVE ID: CVE-2024-44112**		
Affected Version(s): 804					
Missing Authorization	10-Sep-2024	4.3	Due to missing authorization check in SAP for Oil & Gas (Transportation and Distribution), an attacker authenticated as a non-administrative user could call a remote-enabled function which will allow them to delete non-sensitive entries in a user data table. There is no effect on confidentiality or availability. **CVE ID: CVE-2024-44112**	https://url.sap/sapsecuritypatchday	A-SAP-OIL_-180924/478
Affected Version(s): 805					
Missing Authorization	10-Sep-2024	4.3	Due to missing authorization check in SAP for Oil & Gas (Transportation and Distribution), an attacker authenticated as a non-administrative user could call a remote-enabled	https://url.sap/sapsecuritypatchday	A-SAP-OIL_-180924/479

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
			function which will allow them to delete non-sensitive entries in a user data table. There is no effect on confidentiality or availability. **CVE ID: CVE-2024-44112**		
Affected Version(s): 806					
Missing Authorization	10-Sep-2024	4.3	Due to missing authorization check in SAP for Oil & Gas (Transportation and Distribution), an attacker authenticated as a non-administrative user could call a remote-enabled function which will allow them to delete non-sensitive entries in a user data table. There is no effect on confidentiality or availability. **CVE ID: CVE-2024-44112**	https://url.sap/sapsecuritypatchday	A-SAP-OIL_-180924/480
Affected Version(s): 807					
Missing Authorization	10-Sep-2024	4.3	Due to missing authorization check in SAP for Oil & Gas (Transportation and Distribution), an attacker authenticated as a non-administrative	https://url.sap/sapsecuritypatchday	A-SAP-OIL_-180924/481

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
			user could call a remote-enabled function which will allow them to delete non-sensitive entries in a user data table. There is no effect on confidentiality or availability. **CVE ID: CVE-2024-44112**		
Vendor: scriptonite					
Product: music_request_manager					
Affected Version(s): * Up to (including) 1.3					
Cross-Site Request Forgery (CSRF)	12-Sep-2024	6.1	The Music Request Manager WordPress plugin through 1.3 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack **CVE ID: CVE-2024-6017**	N/A	A-SCR-MUSI-180924/482
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Sep-2024	6.1	The Music Request Manager WordPress plugin through 1.3 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute,	N/A	A-SCR-MUSI-180924/483

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
			which could lead to Reflected Cross-Site Scripting in old web browsers **CVE ID: CVE-2024-6018**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Sep-2024	6.1	The Music Request Manager WordPress plugin through 1.3 does not sanitise and escape incoming music requests, which could allow unauthenticated users to perform Cross-Site Scripting attacks against administrators **CVE ID: CVE-2024-6019**	N/A	A-SCR-MUSI-180924/484
Vendor: seacms					
Product: seacms					
Affected Version(s): 12.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Sep-2024	9.8	SeaCMS v12.9 was discovered to contain a SQL injection vulnerability via the id parameter at /dmplayer/dmku/index.php?ac=del. **CVE ID: CVE-2024-44921**	N/A	A-SEA-SEAC-180924/485
Improper Neutralization of Input During Web Page Generation	03-Sep-2024	6.1	A cross-site scripting (XSS) vulnerability in the component admin_collect_news.php of SeaCMS v12.9 allows	N/A	A-SEA-SEAC-180924/486

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
('Cross-site Scripting')			attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the siteurl parameter. **CVE ID: CVE-2024-44920**		
Vendor: semtekyazilim					
Product: semtek_sempos					
Affected Version(s): * Up to (including) 31072024					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Sep-2024	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Semtek Informatics Software Consulting Inc. Semtek Sempos allows Blind SQL Injection.This issue affects Semtek Sempos: through 31072024. **CVE ID: CVE-2024-7076**	N/A	A-SEM-SEMT-180924/487
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Sep-2024	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Semtek Informatics Software Consulting Inc. Semtek Sempos allows SQL	N/A	A-SEM-SEMT-180924/488

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
			Injection.This issue affects Semtek Sempos: through 31072024. **CVE ID: CVE-2024-7078**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Sep-2024	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Semtek Informatics Software Consulting Inc. Semtek Sempos allows Reflected XSS.This issue affects Semtek Sempos: through 31072024. **CVE ID: CVE-2024-7077**	N/A	A-SEM-SEMT-180924/489
Vendor: share-this-image					
Product: share_this_image					
Affected Version(s): * Up to (excluding) 2.03					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Sep-2024	5.4	The Share This Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's STI Buttons shortcode in all versions up to, and including, 2.02 due to insufficient input sanitization and output escaping on user supplied attributes.	https://plugins.trac.wordpress.org/changeset/3146524/	A-SHA-SHAR-180924/490

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
			This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-8363**		
Vendor: Siemens					
Product: sinema_remote_connect_client					
Affected Version(s): * Up to (excluding) 3.2					
Insertion of Sensitive Information into Log File	10-Sep-2024	5.5	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.2 SP2). The affected application inserts sensitive information into a log file which is readable by all legitimate users of the underlying system. This could allow an authenticated attacker to compromise the confidentiality of other users' configuration data. **CVE ID: CVE-2024-42344**	https://cert-portal.siemens.com/productcert/html/ssa-417159.html	A-SIE-SINE-180924/491
Affected Version(s): 3.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	10-Sep-2024	5.5	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.2 SP2). The affected application inserts sensitive information into a log file which is readable by all legitimate users of the underlying system. This could allow an authenticated attacker to compromise the confidentiality of other users' configuration data. **CVE ID: CVE-2024-42344**	https://cert-portal.siemens.com/productcert/html/ssa-417159.html	A-SIE-SINE-180924/492
Product: sinema_remote_connect_server					
Affected Version(s): * Up to (excluding) 3.2					
Session Fixation	10-Sep-2024	4.3	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP2). The affected application does not properly handle user session establishment and invalidation. This could allow a remote attacker to circumvent the additional multi factor authentication for	https://cert-portal.siemens.com/productcert/html/ssa-869574.html	A-SIE-SINE-180924/493

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
			user session establishment. **CVE ID: CVE-2024-42345**		
Affected Version(s): 3.2					
Session Fixation	10-Sep-2024	4.3	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP2). The affected application does not properly handle user session establishment and invalidation. This could allow a remote attacker to circumvent the additional multi factor authentication for user session establishment. **CVE ID: CVE-2024-42345**	https://cert-portal.siemens.com/productcert/html/ssa-869574.html	A-SIE-SINE-180924/494
Vendor: Solarwinds					
Product: access_rights_manager					
Affected Version(s): * Up to (excluding) 2024.3.1					
Use of Hard-coded Credentials	12-Sep-2024	9.8	SolarWinds Access Rights Manager (ARM) was found to contain a hard-coded credential authentication bypass vulnerability. If exploited, this vulnerability would allow access to the RabbitMQ	https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-28990	A-SOL-ACCE-180924/495

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
			management console. We thank Trend Micro Zero Day Initiative (ZDI) for its ongoing partnership in coordinating with SolarWinds on responsible disclosure of this and other potential vulnerabilities. **CVE ID: CVE-2024-28990**		
N/A	12-Sep-2024	8.8	SolarWinds Access Rights Manager (ARM) was found to be susceptible to a remote code execution vulnerability. If exploited, this vulnerability would allow an authenticated user to abuse the service, resulting in remote code execution. **CVE ID: CVE-2024-28991**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-28991	A-SOL-ACCE-180924/496
Vendor: squaredup					
Product: squaredup_ds_for_scom					
Affected Version(s): * Up to (excluding) 6.3.0					
Improper Neutralization of Input During Web Page	03-Sep-2024	5.4	SquaredUp DS for SCOM 6.2.1.11104 allows XSS.	https://scomsupport.squaredup.com/reference/security-advisory/cve-	A-SQU-SQUA-180924/497

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
Generation ('Cross-site Scripting')			**CVE ID: CVE-2024-45180**	2024-45180-stored-cross-site-scripting-knowledge-editor-tile	
Vendor: symphonyfintech					
Product: xts_mobile_trader					
Affected Version(s): 2.0.0.1					
N/A	03-Sep-2024	8.8	This vulnerability exists due to improper access controls on APIs in the Authentication module of Symphony XTS Web Trading and Mobile Trading platforms (version 2.0.0.1_P160). An authenticated remote attacker could exploit this vulnerability by manipulating parameters through HTTP request which could lead to unauthorized account take over belonging to other users. **CVE ID: CVE-2024-45586**	N/A	A-SYM-XTS_-180924/498
N/A	03-Sep-2024	8.8	This vulnerability exists in Symphony XTS Web Trading platform version 2.0.0.1_P160 due to improper access controls on APIs in the Transaction	N/A	A-SYM-XTS_-180924/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module of vulnerable application. An authenticated remote attacker could exploit this vulnerability by manipulating parameters through HTTP request which could lead to compromise of other user accounts. **CVE ID: CVE-2024-45587**		
Incorrect Authorization	03-Sep-2024	8.1	This vulnerability exists in Symphony XTS Web Trading platform version 2.0.0.1_P160 due to improper access controls on APIs in the Preference module of the application. An authenticated remote attacker could exploit this vulnerability by manipulating parameters through HTTP request which could lead to unauthorized access and modification of sensitive information belonging to other users.	N/A	A-SYM-XTS_-180924/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45588		
Product: xts_web_trader					
Affected Version(s): 2.0.0.1					
N/A	03-Sep-2024	8.8	This vulnerability exists due to improper access controls on APIs in the Authentication module of Symphony XTS Web Trading and Mobile Trading platforms (version 2.0.0.1_P160). An authenticated remote attacker could exploit this vulnerability by manipulating parameters through HTTP request which could lead to unauthorized account take over belonging to other users. **CVE ID: CVE-2024-45586**	N/A	A-SYM-XTS_-180924/501
N/A	03-Sep-2024	8.8	This vulnerability exists in Symphony XTS Web Trading platform version 2.0.0.1_P160 due to improper access controls on APIs in the Transaction module of vulnerable application. An authenticated	N/A	A-SYM-XTS_-180924/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker could exploit this vulnerability by manipulating parameters through HTTP request which could lead to compromise of other user accounts. **CVE ID: CVE-2024-45587**		
Incorrect Authorization	03-Sep-2024	8.1	This vulnerability exists in Symphony XTS Web Trading platform version 2.0.0.1_P160 due to improper access controls on APIs in the Preference module of the application. An authenticated remote attacker could exploit this vulnerability by manipulating parameters through HTTP request which could lead to unauthorized access and modification of sensitive information belonging to other users. **CVE ID: CVE-2024-45588**	N/A	A-SYM-XTS_-180924/503
Vendor: Syspass					

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
Product: syspass					
Affected Version(s): From (including) 3.2.0 Up to (including) 3.2.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	6.1	A cross-site scripting (XSS) vulnerability in SysPass 3.2.x allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the name parameter at /Controllers/ClientController.php. **CVE ID: CVE-2024-42904**	N/A	A-SYS-SYSP-180924/504
Vendor: themetechmount					
Product: truebooker					
Affected Version(s): * Up to (including) 1.0.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Sep-2024	9.8	The TrueBooker WordPress plugin before 1.0.3 does not properly sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection. **CVE ID: CVE-2024-6924**	N/A	A-THE-TRUE-180924/505
Cross-Site Request Forgery (CSRF)	08-Sep-2024	4.3	The TrueBooker WordPress plugin before 1.0.3 does not have CSRF check in place when updating its	N/A	A-THE-TRUE-180924/506

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
			settings, which could allow attackers to make a logged in admin change them via a CSRF attack. **CVE ID: CVE-2024-6925**		
Vendor: thimpress					
Product: learnpress					
Affected Version(s): * Up to (excluding) 4.2.7.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.5	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to SQL Injection via the 'c_only_fields' parameter of the /wp-json/learnpress/v1/courses REST API endpoint in all versions up to, and including, 4.2.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive	N/A	A-THI-LEAR-180924/507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information from the database. **CVE ID: CVE-2024-8522**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Sep-2024	7.5	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to SQL Injection via the 'c_fields' parameter of the /wp-json/lp/v1/courses/archive-course REST API endpoint in all versions up to, and including, 4.2.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2024-8529**	https://plugins.trac.wordpress.org/changeset?old_path=/learnpress/tags/4.2.7&new_path=/learnpress/tags/4.2.7.1&sfp_email=&sfph_mail=	A-THI-LEAR-180924/508
Vendor: ti					
Product: fusion_digital_power_designer					
Affected Version(s): 7.10.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	12-Sep-2024	5.5	An issue in Texas Instruments Fusion Digital Power Designer v.7.10.1 allows a local attacker to obtain sensitive information via the plaintext storage of credentials **CVE ID: CVE-2024-41629**	N/A	A-TI-FUSI-180924/509
Vendor: tina					
Product: tina					
Affected Version(s): * Up to (excluding) 1.6.2					
Cleartext Storage of Sensitive Information	03-Sep-2024	7.5	Tina is an open-source content management system (CMS). Sites building with Tina CMS's command line interface (CLI) prior to version 1.6.2 that use a search token may be vulnerable to the search token being leaked via lock file (tina-lock.json). Administrators of Tina-enabled websites with search setup should rotate their key immediately. This issue has been patched in @tinacms/cli version 1.6.2. Upgrading and rotating the search	https://github.com/tinacms/tinacms/commit/110f1ceea4574d636a64526648f7c8bf6539b26a, https://github.com/tinacms/tinacms/security/advisories/GHSA-4qrm-9h4r-v2fx	A-TIN-TINA-180924/510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			token is required for the proper fix. **CVE ID: CVE-2024-45391**		
Vendor: tmsproducts					
Product: amelia					
Affected Version(s): * Up to (including) 1.2.3					
Missing Authorization	05-Sep-2024	6.5	The Booking for Appointments and Events Calendar – Amelia Premium and Lite plugins for WordPress are vulnerable to unauthorized access of data due to a missing capability check on the 'ameliaButtonCommand' function in all versions up to, and including, Premium 7.7 and Lite 1.2.3. This makes it possible for unauthenticated attackers to access employee calendar details, including Google Calendar OAuth tokens in the premium version. **CVE ID: CVE-2024-6332**	N/A	A-TMS-AMEL-180924/511
Affected Version(s): * Up to (including) 7.7					
Missing Authorization	05-Sep-2024	6.5	The Booking for Appointments and Events Calendar – Amelia Premium	N/A	A-TMS-AMEL-180924/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Lite plugins for WordPress are vulnerable to unauthorized access of data due to a missing capability check on the 'ameliaButtonCommand' function in all versions up to, and including, Premium 7.7 and Lite 1.2.3. This makes it possible for unauthenticated attackers to access employee calendar details, including Google Calendar OAuth tokens in the premium version. **CVE ID: CVE-2024-6332**		
Vendor: trellix					
Product: intrusion_prevention_system_manager					
Affected Version(s): * Up to (excluding) 11.1.7.97					
Improper Authentication	05-Sep-2024	7.5	This vulnerability allows unauthenticated remote attackers to bypass authentication and gain APIs access of the Manager. **CVE ID: CVE-2024-5957**	N/A	A-TRE-INTR-180924/513
Affected Version(s): 11.1.7.97					

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 Authentication	05-Sep-2024	5.3	This vulnerability allows unauthenticated remote attackers to bypass authentication and gain partial data access to the vulnerable Trellix IPS Manager with garbage data in response mostly **CVE ID: CVE-2024-5956**	N/A	A-TRE-INTR-180924/514
Vendor: ultimaker					
Product: ultimaker_cura					
Affected Version(s): 5.7.0					
Improper Control of Generation of Code ('Code Injection')	03-Sep-2024	7.8	UltiMaker Cura slicer versions 5.7.0-beta.1 through 5.7.2 are vulnerable to code injection via the 3MF format reader (/plugins/ThreeMFReader.py). The vulnerability arises from improper handling of the drop_to_buildplate property within 3MF files, which are ZIP archives containing the model data. When a 3MF file is loaded in Cura, the value of the drop_to_buildplate property is passed to the Python eval() function without	https://github.com/Ultimaker/Cura/commit/285a241eb28da3188c977f85d68937c0dad79c50	A-ULT-ULTI-180924/515

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
			proper sanitization, allowing an attacker to execute arbitrary code by crafting a malicious 3MF file. This vulnerability poses a significant risk as 3MF files are commonly shared via 3D model databases. **CVE ID: CVE-2024-8374**		
Affected Version(s): 5.7.1					
Improper Control of Generation of Code ('Code Injection')	03-Sep-2024	7.8	UltiMaker Cura slicer versions 5.7.0-beta.1 through 5.7.2 are vulnerable to code injection via the 3MF format reader (/plugins/ThreeMFReader.py). The vulnerability arises from improper handling of the drop_to_buildplate property within 3MF files, which are ZIP archives containing the model data. When a 3MF file is loaded in Cura, the value of the drop_to_buildplate property is passed to the Python eval() function without proper sanitization, allowing an attacker to execute	https://github.com/Ultimaker/Cura/commit/285a241eb28da3188c977f85d68937c0dad79c50	A-ULT-ULTI-180924/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code by crafting a malicious 3MF file. This vulnerability poses a significant risk as 3MF files are commonly shared via 3D model databases. **CVE ID: CVE-2024-8374**		
Affected Version(s): 5.7.2					
Improper Control of Generation of Code ('Code Injection')	03-Sep-2024	7.8	UltiMaker Cura slicer versions 5.7.0-beta.1 through 5.7.2 are vulnerable to code injection via the 3MF format reader (/plugins/ThreeMFReader.py). The vulnerability arises from improper handling of the drop_to_buildplate property within 3MF files, which are ZIP archives containing the model data. When a 3MF file is loaded in Cura, the value of the drop_to_buildplate property is passed to the Python eval() function without proper sanitization, allowing an attacker to execute arbitrary code by crafting a malicious 3MF file. This	https://github.com/Ultimaker/Cura/commit/285a241eb28da3188c977f85d68937c0dad79c50	A-ULT-ULTI-180924/517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability poses a significant risk as 3MF files are commonly shared via 3D model databases. **CVE ID: CVE-2024-8374**		
Affected Version(s): 5.8.0					
Improper Control of Generation of Code ('Code Injection')	03-Sep-2024	7.8	UltiMaker Cura slicer versions 5.7.0-beta.1 through 5.7.2 are vulnerable to code injection via the 3MF format reader (/plugins/ThreeMFReader.py). The vulnerability arises from improper handling of the drop_to_buildplate property within 3MF files, which are ZIP archives containing the model data. When a 3MF file is loaded in Cura, the value of the drop_to_buildplate property is passed to the Python eval() function without proper sanitization, allowing an attacker to execute arbitrary code by crafting a malicious 3MF file. This vulnerability poses a significant risk as 3MF files are	https://github.com/Ultimaker/Cura/commit/285a241eb28da3188c977f85d68937c0dad79c50	A-ULT-ULTI-180924/518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commonly shared via 3D model databases. **CVE ID: CVE-2024-8374**		
Vendor: uniong					
Product: webitr					
Affected Version(s): * Up to (excluding) 2_1_0_28					
URL Redirection to Untrusted Site ('Open Redirect')	09-Sep-2024	6.1	WebITR from Uniong has an Open Redirect vulnerability, which allows unauthorized remote attackers to exploit this vulnerability to forge URLs. Users, believing they are accessing a trusted domain, can be redirected to another page, potentially leading to phishing attacks. **CVE ID: CVE-2024-8586**	N/A	A-UNI-WEBI-180924/519
Vendor: virtualmin					
Product: virtualmin					
Affected Version(s): * Up to (excluding) 7.20.2					
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Sep-2024	7.5	Webmin before 2.202 and Virtualmin before 7.20.2 allow a network traffic loop via spoofed UDP packets on port 10000. **CVE ID: CVE-2024-45692**	N/A	A-VIR-VIRT-180924/520

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
Vendor: Webmin					
Product: webmin					
Affected Version(s): * Up to (excluding) 2.202					
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Sep-2024	7.5	Webmin before 2.202 and Virtualmin before 7.20.2 allow a network traffic loop via spoofed UDP packets on port 10000. **CVE ID: CVE-2024-45692**	N/A	A-WEB-WEBM-180924/521
Vendor: wpeka					
Product: wp_adcenter					
Affected Version(s): * Up to (excluding) 2.5.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	The WP AdCenter – Ad Manager & Adsense Ads plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ad_alignment' attribute in all versions up to, and including, 2.5.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a	https://plugins.trac.wordpress.org/changeset/3146736/, https://plugins.trac.wordpress.org/changeset/3146736/#file6	A-WPE-WP_A-180924/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user accesses an injected page. **CVE ID: CVE-2024-8317**		
Vendor: wpengine					
Product: advanced_custom_fields					
Affected Version(s): * Up to (including) 6.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Sep-2024	6.1	Cross-site scripting vulnerability exists in Advanced Custom Fields versions 6.3.5 and earlier and Advanced Custom Fields Pro versions 6.3.5 and earlier. If an attacker with the 'capability' setting privilege which is set in the product settings stores an arbitrary script in the field label, the script may be executed on the web browser of the logged-in user with the same privilege as the attacker's. **CVE ID: CVE-2024-45429**	N/A	A-WPE-ADVA-180924/523
Vendor: wpextended					
Product: wp_extended					
Affected Version(s): * Up to (excluding) 3.0.9					
Missing Authorization	04-Sep-2024	8.8	The The Ultimate WordPress Toolkit – WP Extended plugin for WordPress is vulnerable to	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=31	A-WPE-WP_E-180924/524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the module_all_toggle_ajax() function in all versions up to, and including, 3.0.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update arbitrary options on the WordPress site. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site. **CVE ID: CVE-2024-8102**	45430%40wpextended%2Ftrunk&old=3134345%40wpextended%2Ftrunk&sfp_email=&sfph_mail=	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Sep-2024	6.5	The The Ultimate WordPress Toolkit – WP Extended plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 3.0.8 via the	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3145430%40wpextended%2Ftrunk&old=3134345%40wpextend	A-WPE-WP_E-180924/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			download_file_ajax function. This makes it possible for authenticated attackers, with subscriber access and above, to read the contents of arbitrary files on the server, which can contain sensitive information. **CVE ID: CVE-2024-8104**	ed%2Ftrunk&sfp_email=&sfph_mail=	
N/A	04-Sep-2024	6.5	The The Ultimate WordPress Toolkit – WP Extended plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.0.8 via the download_user_ajax function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to extract sensitive data including usernames, hashed passwords, and emails. **CVE ID: CVE-2024-8106**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3145430%40wpextended%2Ftrunk&old=3134345%40wpextended%2Ftrunk&sfp_email=&sfph_mail=	A-WPE-WP_E-180924/526

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 Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Sep-2024	6.1	The The Ultimate WordPress Toolkit – WP Extended plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'selected_option' parameter in all versions up to, and including, 3.0.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-8117**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3145430%40wpextended%2Ftrunk&old=3134345%40wpextended%2Ftrunk&sfp_email=&sfph_mail=	A-WPE-WP_E-180924/527
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Sep-2024	6.1	The The Ultimate WordPress Toolkit – WP Extended plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the page parameter in all versions up to, and including, 3.0.8 due to insufficient input sanitization	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3145430%40wpextended%2Ftrunk&old=3134345%40wpextended%2Ftrunk&sfp_email=&sfph_mail=	A-WPE-WP_E-180924/528

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
			and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-8119**		
Authorization Bypass Through User-Controlled Key	04-Sep-2024	5.4	The The Ultimate WordPress Toolkit – WP Extended plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.0.8 via the duplicate_post function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Contributor-level access and above, to duplicate posts written by other authors including admins. This includes the ability to duplicate	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3145430%40wpextended%2Ftrunk&old=3134345%40wpextended%2Ftrunk&sfp_email=&sfph_mail=	A-WPE-WP_E-180924/529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password-protected posts, which reveals their contents. **CVE ID: CVE-2024-8123**		
Missing Authorization	04-Sep-2024	4.3	The The Ultimate WordPress Toolkit – WP Extended plugin for WordPress is vulnerable to unauthorized modification of user names due to a missing capability check on the wpext_change_admin_name() function in all versions up to, and including, 3.0.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change an admin's username to a username of their liking as long as the default 'admin' was used. **CVE ID: CVE-2024-8121**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3145430%40wpextended%2Ftrunk&old=3134345%40wpextended%2Ftrunk&sfp_email=&sfph_mail=	A-WPE-WP_E-180924/530
Vendor: wpshuffle					
Product: frontend_post_submission_manager					
Affected Version(s): * Up to (excluding) 1.2.3					
Missing Authorization	06-Sep-2024	4.3	The Frontend Post Submission Manager Lite – Frontend Posting	https://plugins.trac.wordpress.org/changeset/3147218/fronte	A-WPS-FRON-180924/531

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
			WordPress Plugin plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_global_settings and process_form_edit functions in all versions up to, and including, 1.2.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the plugin's settings and forms. **CVE ID: CVE-2024-8427**	nd-post-submission-manager-lite/trunk/includes/classes/admin/class-fpsml-ajax-admin.php	
Vendor: wpvibes					
Product: form_vibes					
Affected Version(s): * Up to (excluding) 1.4.13					
Missing Authorization	05-Sep-2024	5.4	The Form Vibes – Database Manager for Forms plugin for WordPress is vulnerable to unauthorized access of data and modification of data due to a missing capability check on the fv_export_csv, reset_settings,	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3128705%40form-vibes&new=3128705%40form-vibes&sfp_email=&sfph_mail=	A-WPV-FORM-180924/532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			save_settings, save_columns_settings, get_analytics_data, get_event_logs_data, delete_submissions, and get_submissions functions in all versions up to, and including, 1.4.12. This makes it possible for authenticated attackers, with Subscriber-level access and above, to perform multiple unauthorized actions. NOTE: This vulnerability is partially fixed in version 1.4.12. **CVE ID: CVE-2024-5309**		
Vendor: xibosignage					
Product: xibo					
Affected Version(s): * Up to (excluding) 4.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	5.4	Xibo is an open source digital signage platform with a web content management system (CMS). Prior to version 4.1.0, a cross-site scripting vulnerability in Xibo CMS allows authorized users to execute arbitrary	https://github.com/xibosignage/xibo-cms/commit/d8f13339469d9f19ce591fb2bd7c9e0e0d2da118, https://github.com/xibosignage/xibo-cms/security/advisories/GHSA	A-XIB-XIBO-180924/533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript via the file preview function. Users can upload HTML/CSS/JS files into the Xibo Library via the Generic File module to be referenced on Displays and in Layouts. This is intended functionality. When previewing these resources from the Library and Layout editor they are executed in the users browser. This will be disabled in future releases, and users are encouraged to use the new developer tools in 4.1 to design their widgets which require this type of functionality. This behavior has been changed in 4.1.0 to preview previewing of generic files. There are no workarounds for this issue. **CVE ID: CVE-2024-43412**	-336f-wrgx-57gg	
Improper Neutralization of Input	03-Sep-2024	4.8	Xibo is an open source digital signage platform	https://github.com/xibosignage/xibo-	A-XIB-XIBO-180924/534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			with a web content management system (CMS). Prior to version 4.1.0, a cross-site scripting vulnerability in Xibo CMS allows authorized users to execute JavaScript via the DataSet functionality. Users can design a DataSet with a HTML column which contains JavaScript, which is intended functionality. The JavaScript gets executed on the Data Entry page and in any Layouts which reference it. This behavior has been changed in 4.1.0 to show HTML/CSS/JS as code on the Data Entry page. There are no workarounds for this issue. **CVE ID: CVE-2024-43413**	cms/commit/009527855d8bfd0ffb95f5c88ed72b7b5bdebfa1, https://github.com/xibosignage/xibo-cms/security/advisories/GHSA-pfxp-vxh7-2h9f	
Vendor: Yandex					
Product: yandex_browser					
Affected Version(s): * Up to (excluding) 24.7.1.380					
Untrusted Search Path	03-Sep-2024	7.8	Yandex Browser for Desktop before 24.7.1.380 has a DLL Hijacking	https://yandex.com/bugbounty/i/hall-of-fame-browser/	A-YAN-YAND-180924/535

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
			Vulnerability because an untrusted search path is used. **CVE ID: CVE-2024-6473**		
Vendor: zzcms					
Product: zzcms					
Affected Version(s): * Up to (including) 2023					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Sep-2024	6.1	Cross Site Scripting vulnerability in ZZCMS v.2023 and before allows a remote attacker to obtain sensitive information via a crafted script to the pagename parameter of the admin/del.php component. **CVE ID: CVE-2024-44819**	N/A	A-ZZC-ZZCM-180924/536
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Sep-2024	6.1	A sensitive information disclosure vulnerability exists in ZZCMS v.2023 and before within the eginfo.php file located at /3/E_bak5.1/upload/. When accessed with the query parameter phome=ShowPHPInfo, the application executes the phpinfo() function, which exposes detailed information about	N/A	A-ZZC-ZZCM-180924/537

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 PHP environment, including server configuration, loaded modules, and environment variables. **CVE ID: CVE-2024-44820**		
Hardware					
Vendor: comfast					
Product: cf-xr11					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Sep-2024	9.8	COMFAST CF-XR11 V2.7.2 has a command injection vulnerability in function sub_424CB4. Attackers can send POST request messages to /usr/bin/webmgnt and inject commands into parameter iface. **CVE ID: CVE-2024-44466**	N/A	H-COM-CF-X-180924/538
Vendor: crucial					
Product: ct1000mx500ssd1					
Affected Version(s): -					
Out-of-bounds Write	04-Sep-2024	6.7	Micron Crucial MX500 Series Solid State Drives M3CR046 is vulnerable to Buffer Overflow, which can be triggered by sending specially	N/A	H-CRU-CT10-180924/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted ATA packets from the host to the drive controller. **CVE ID: CVE-2024-42642**		
Product: ct2000mx500ssd1					
Affected Version(s): -					
Out-of-bounds Write	04-Sep-2024	6.7	Micron Crucial MX500 Series Solid State Drives M3CR046 is vulnerable to Buffer Overflow, which can be triggered by sending specially crafted ATA packets from the host to the drive controller. **CVE ID: CVE-2024-42642**	N/A	H-CRU-CT20-180924/540
Product: ct250mx500ssd1					
Affected Version(s): -					
Out-of-bounds Write	04-Sep-2024	6.7	Micron Crucial MX500 Series Solid State Drives M3CR046 is vulnerable to Buffer Overflow, which can be triggered by sending specially crafted ATA packets from the host to the drive controller. **CVE ID: CVE-2024-42642**	N/A	H-CRU-CT25-180924/541

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
Product: ct4000mx500ssd1					
Affected Version(s): -					
Out-of-bounds Write	04-Sep-2024	6.7	Micron Crucial MX500 Series Solid State Drives M3CR046 is vulnerable to Buffer Overflow, which can be triggered by sending specially crafted ATA packets from the host to the drive controller. **CVE ID: CVE-2024-42642**	N/A	H-CRU-CT40-180924/542
Product: ct500mx500ssd1					
Affected Version(s): -					
Out-of-bounds Write	04-Sep-2024	6.7	Micron Crucial MX500 Series Solid State Drives M3CR046 is vulnerable to Buffer Overflow, which can be triggered by sending specially crafted ATA packets from the host to the drive controller. **CVE ID: CVE-2024-42642**	N/A	H-CRU-CT50-180924/543
Vendor: Dell					
Product: 7920_xl					
Affected Version(s): -					
Improper Restriction of	10-Sep-2024	5.5	Dell Precision Rack, 14G Intel BIOS versions prior to	https://www.dell.com/support/kbdoc/en-	H-DEL-7920-180924/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			2.22.2, contains an Access of Memory Location After End of Buffer vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure. **CVE ID: CVE-2024-42425**	us/000227015/dsa-2024-328	
Product: precision_7920					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Sep-2024	5.5	Dell Precision Rack, 14G Intel BIOS versions prior to 2.22.2, contains an Access of Memory Location After End of Buffer vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure. **CVE ID: CVE-2024-42425**	https://www.dell.com/support/kbdoc/en-us/000227015/dsa-2024-328	H-DEL-PREC-180924/545
Vendor: Dlink					
Product: di-8100g					
Affected Version(s): -					
Improper Neutralization of	06-Sep-2024	9.8	D-Link DI-8100G 17.12.20A1 is vulnerable to	N/A	H-DLI-DI-8-180924/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			Command Injection via sub47A60C function in the upgrade_filter.asp file **CVE ID: CVE-2024-44401**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Sep-2024	9.8	D-Link DI-8100G 17.12.20A1 is vulnerable to Command Injection via msp_info.htm. **CVE ID: CVE-2024-44402**	N/A	H-DLI-DI-8-180924/547
Product: di-8300					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-Sep-2024	9.8	D-Link DI-8300 v16.07.26A1 is vulnerable to command injection via the upgrade_filter_asp function. **CVE ID: CVE-2024-44410**	N/A	H-DLI-DI-8-180924/548
Product: di-8400					
Affected Version(s): a1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Sep-2024	9.8	D-Link DI-8400 16.07.26A1 is vulnerable to Command Injection via upgrade_filter_asp. **CVE ID: CVE-2024-44400**	N/A	H-DLI-DI-8-180924/549

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
Product: dir-823g					
Affected Version(s): -					
Missing Authorization	06-Sep-2024	7.5	D-Link DIR-823G v1.0.2B05_20181207 is vulnerable to Information Disclosure. The device allows unauthorized configuration file downloads, and the downloaded configuration files contain plaintext user passwords. **CVE ID: CVE-2024-44408**	N/A	H-DLI-DIR--180924/550
Product: dns-320					
Affected Version(s): -					
N/A	05-Sep-2024	5.9	A vulnerability, which was classified as problematic, has been found in D-Link DNS-320 2.02b01. Affected by this issue is some unknown functionality of the file /cgi-bin/widget_api.cgi of the component Web Management Interface. The manipulation of the argument getHD/getSer/getSys leads to information disclosure. The attack may be launched remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--180924/551

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 complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8460**		
N/A	05-Sep-2024	5.3	A vulnerability, which was classified as problematic, was found in D-Link DNS-320 2.02b01. This affects an unknown part of the file /cgi-bin/discovery.cgi of the component Web Management Interface. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The exploit has been	N/A	H-DLI-DNS--180924/552

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
			disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8461**		
Vendor: Draytek					
Product: vigor3900					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	DrayTek Vigor3900 v1.5.1.6 was discovered to contain an authenticated command injection vulnerability via the name parameter in the run_command function. **CVE ID: CVE-2024-44844**	N/A	H-DRA-VIGO-180924/553
Improper Neutralization of Special Elements used in an OS Command ('OS	06-Sep-2024	8.8	DrayTek Vigor3900 v1.5.1.6 was discovered to contain an authenticated command injection vulnerability via the value parameter in the	N/A	H-DRA-VIGO-180924/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			filter_string function. **CVE ID: CVE-2024-44845**		
Vendor: kasdanet					
Product: kw5515					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Sep-2024	4.3	Cross Site Scripting (XSS) Vulnerability in Firewall menu in Control Panel in KASDA KW5515 version 4.3.1.0, allows attackers to execute arbitrary code and steal cookies via a crafted script **CVE ID: CVE-2020-24061**	N/A	H-KAS-KW55-180924/555
Vendor: Linksys					
Product: wrt54g					
Affected Version(s): -					
Out-of-bounds Write	04-Sep-2024	9.8	A vulnerability was found in Linksys WRT54G 4.21.5. It has been rated as critical. Affected by this issue is the function validate_services_port of the file /apply.cgi of the component POST Parameter Handler. The manipulation of the argument services_array leads to stack-based buffer	N/A	H-LIN-WRT5-180924/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow. 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-2024-8408**		
Vendor: mediatek					
Product: mt6580					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT65-180924/557
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT65-180924/558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Product: mt6739					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/559
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/560

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
			User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Product: mt6761					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/561
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204;	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/562

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
			Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Product: mt6765					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1551. **CVE ID: CVE-2024-20086**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/563
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1550.	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/564

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
			CVE ID: CVE-2024-20087		
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/565
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/566
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT67-180924/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	bulletin/September-2024	
Product: mt6768					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1551. **CVE ID: CVE-2024-20086**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/568
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/569

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
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1550. **CVE ID: CVE-2024-20087**		
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/570
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204;	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/571

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
			Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/572
Product: mt6779					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1551.	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20086		
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1550. **CVE ID: CVE-2024-20087**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/574
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/575
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT67-180924/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	bulletin/September-2024	
Product: mt6781					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/577
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/579
Product: mt6785					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1551. **CVE ID: CVE-2024-20086**		
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1550. **CVE ID: CVE-2024-20087**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/581
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/582

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
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/583
Product: mt6789					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT67-180924/584
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT67-180924/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	bulletin/September-2024	
Product: mt6833					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/586
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/587

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
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/588
Product: mt6835					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/589

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
			not needed for exploitation. Patch ID: ALPS08861558; Issue ID: MSV-1526. **CVE ID: CVE-2024-20089**		
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/590
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560.	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/591

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
			CVE ID: CVE-2024-20085		
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/592
Product: mt6853					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/593

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
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/594
Product: mt6855					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/595
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-180924/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	bulletin/September-2024	
Product: mt6873					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/597
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/598

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
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Product: mt6877					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/599
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/601
Product: mt6878					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558;	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MSV-1526. **CVE ID: CVE-2024-20089**		
Product: mt6879					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/603
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560.	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20085		
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/605
Product: mt6880					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/606

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
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/607
Product: mt6883					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/608
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-180924/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	bulletin/September-2024	
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/610
Product: mt6885					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/611

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
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**		
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/612
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099;	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/613

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
			Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**		
Product: mt6886					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558; Issue ID: MSV-1526. **CVE ID: CVE-2024-20089**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/614
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561.	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20084		
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/616
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/617
Product: mt6889					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/618
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/619
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/620

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
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**		
Product: mt6890					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/621
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Product: mt6893					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/623
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204;	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/624

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
			Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/625
Product: mt6895					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561.	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20084		
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/627
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/628
Product: mt6897					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558; Issue ID: MSV-1526. **CVE ID: CVE-2024-20089**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/629
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/630
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/631

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
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT68-180924/632
Product: mt6980					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT69-180924/633

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
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558; Issue ID: MSV-1526. **CVE ID: CVE-2024-20089**		
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT69-180924/634
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204;	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT69-180924/635

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
			Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Product: mt6983					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT69-180924/636
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560.	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT69-180924/637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20085		
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT69-180924/638
Product: mt6985					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558; Issue ID: MSV-1526. **CVE ID: CVE-2024-20089**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT69-180924/639

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
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT69-180924/640
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT69-180924/641
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT69-180924/642

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
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**		
Product: mt6989					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558; Issue ID: MSV-1526. **CVE ID: CVE-2024-20089**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT69-180924/643
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT69-180924/644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**		
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT69-180924/645
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543.	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT69-180924/646

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
			CVE ID: CVE-2024-20088		
Product: mt6990					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558; Issue ID: MSV-1526. **CVE ID: CVE-2024-20089**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT69-180924/647
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT69-180924/648

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
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT69-180924/649
Product: mt8183					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT81-180924/650
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT81-180924/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	bulletin/September-2024	
Product: mt8188					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT81-180924/652
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT81-180924/653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Product: mt8195					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT81-180924/654
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT81-180924/655

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
			exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Product: mt8321					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT83-180924/656
Product: mt8385					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT83-180924/657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS08932916; Issue ID: MSV-1551. **CVE ID: CVE-2024-20086**		
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1550. **CVE ID: CVE-2024-20087**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT83-180924/658
Product: mt8390					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561.	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT83-180924/659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-20084		
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT83-180924/660
Product: mt8395					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT83-180924/661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT83-180924/662
Product: mt8666					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1551. **CVE ID: CVE-2024-20086**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT86-180924/663
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT86-180924/664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1550. **CVE ID: CVE-2024-20087**	bulletin/September-2024	
Product: mt8667					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1551. **CVE ID: CVE-2024-20086**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT86-180924/665
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT86-180924/666

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
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1550. **CVE ID: CVE-2024-20087**		
Product: mt8673					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT86-180924/667
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT86-180924/668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Product: mt8675					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT86-180924/669
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560.	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT86-180924/670

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
			CVE ID: CVE-2024-20085		
Product: mt8676					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT86-180924/671
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT86-180924/672
Product: mt8678					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558; Issue ID: MSV-1526. **CVE ID: CVE-2024-20089**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT86-180924/673
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT86-180924/674
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT86-180924/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	bulletin/September-2024	
Product: mt8755					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/676
Product: mt8765					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/677

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
			lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**		
Product: mt8766					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1551. **CVE ID: CVE-2024-20086**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/678
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1550. **CVE ID: CVE-2024-20087**		
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/680
Product: mt8768					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/681

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
			ID: ALPS08932916; Issue ID: MSV-1551. **CVE ID: CVE-2024-20086**		
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1550. **CVE ID: CVE-2024-20087**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/682
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/683
Product: mt8775					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558; Issue ID: MSV-1526. **CVE ID: CVE-2024-20089**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/684
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/685
Product: mt8781					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1551. **CVE ID: CVE-2024-20086**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/686
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1550. **CVE ID: CVE-2024-20087**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/687
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/688

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
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**		
Product: mt8786					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/689
Product: mt8788					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1551. **CVE ID: CVE-2024-20086**		
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1550. **CVE ID: CVE-2024-20087**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/691
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099;	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/692

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
			Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**		
Product: mt8789					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1551. **CVE ID: CVE-2024-20086**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/693
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1550.	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/694

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
			CVE ID: CVE-2024-20087		
Product: mt8792					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558; Issue ID: MSV-1526. **CVE ID: CVE-2024-20089**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/695
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/696

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
Product: mt8796					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558; Issue ID: MSV-1526. **CVE ID: CVE-2024-20089**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/697
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	H-MED-MT87-180924/698
Vendor: Qualcomm					
Product: 205					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-205-180924/699
Product: 205_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-205_-180924/700
Product: 215					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-215-180924/701
Product: 215_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-215_-180924/702
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/security	H-QUA-215_-180924/703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	bulletin/september-2024-bulletin.html	
Product: 315_5g_iot					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-315_-180924/704
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-315_-180924/705
Product: 9206_lte					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-9206-180924/706
Product: apq8017					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-APQ8-180924/707

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-APQ8-180924/708
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-APQ8-180924/709
Product: aqt1000					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-AQT1-180924/710
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-AQT1-180924/711
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-AQT1-180924/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-AQT1-180924/713
Product: ar8031					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-AR80-180924/714
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-AR80-180924/715
Product: ar8035					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-AR80-180924/716
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-AR80-180924/717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33060	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-AR80-180924/718
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-AR80-180924/719
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-AR80-180924/720
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-AR80-180924/721
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-AR80-180924/722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33051	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-AR80-180924/723
Product: ar9380					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-AR93-180924/724
Product: c-v2x_9150					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-C-V2-180924/725
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-C-V2-180924/726

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
			CVE ID: CVE-2024-38401	bulletin/september-2024-bulletin.html	
Product: csr8811					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-CSR8-180924/727
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-CSR8-180924/728
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-CSR8-180924/729
Product: csra6620					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-CSRA-180924/730
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-CSRA-180924/731
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-CSRA-180924/732
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-CSRA-180924/733
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-CSRA-180924/734
Product: csra6640					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-CSRA-180924/735
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-CSRA-180924/736
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-CSRA-180924/737
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-CSRA-180924/738
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-CSRA-180924/739

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
Product: csrb31024					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-CSRB-180924/740
Product: fastconnect_6200					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/741
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/742
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/743
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/744

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
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/745
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/746
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/747
Product: fastconnect_6700					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/748
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-FAST-180924/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33042	bulletin/september-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/750
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/751
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/752
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/753
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-FAST-180924/754

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
			CVE ID: CVE-2024-33060	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/755
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/756
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/757
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/758
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-FAST-180924/759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: fastconnect_6800					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/760
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/761
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/762
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/764
Product: fastconnect_6900					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/765
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/766
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/767
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/769
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/770
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/771
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/772
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/773

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/774
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/775
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/776
Product: fastconnect_7800					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/777

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/778
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/779
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/780
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/781
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/782
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	H-QUA-FAST-180924/783

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
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/784
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/785
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/786
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/787

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/788
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FAST-180924/789
Product: flight_rb5_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FLIG-180924/790
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FLIG-180924/791
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-FLIG-180924/792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38402	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FLIG-180924/793
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FLIG-180924/794
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FLIG-180924/795
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FLIG-180924/796
Product: fsm10055					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FSM1-180924/797
Product: fsm10056					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FSM1-180924/798
Product: fsm20055					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FSM2-180924/799
Product: fsm20056					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-FSM2-180924/800
Product: home_hub_100					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-HOME-180924/801
Product: immersive_home_214					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IMME-180924/802
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IMME-180924/803
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IMME-180924/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: immersive_home_216					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IMME-180924/805
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IMME-180924/806
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IMME-180924/807
Product: immersive_home_316					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-IMME-180924/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beacon/probe response frame. **CVE ID: CVE-2024-33048**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IMME-180924/809
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IMME-180924/810
Product: immersive_home_318					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IMME-180924/811
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation	https://docs.qualcomm.com/product/publicresources/security	H-QUA-IMME-180924/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IMME-180924/813
Product: immersive_home_3210					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IMME-180924/814
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IMME-180924/815
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-IMME-180924/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IMME-180924/817
Product: immersive_home_326					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IMME-180924/818
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IMME-180924/819
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-IMME-180924/820

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
			length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IMME-180924/821
Product: ipq4018					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ4-180924/822
Product: ipq4019					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ4-180924/823

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
			CVE ID: CVE-2024-33050		
Product: ipq4028					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ4-180924/824
Product: ipq4029					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ4-180924/825
Product: ipq5010					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ5-180924/826

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ5-180924/827
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ5-180924/828
Product: ipq5028					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ5-180924/829
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ5-180924/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ5-180924/831
Product: ipq5300					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ5-180924/832
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ5-180924/833
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when	https://docs.qualcomm.com/product/publicresources/security	H-QUA-IPQ5-180924/834

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
			common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	bulletin/september-2024-bulletin.html	
Product: ipq5302					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ5-180924/835
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ5-180924/836
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ5-180924/837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq5312					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ5-180924/838
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ5-180924/839
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ5-180924/840
Product: ipq5332					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-IPQ5-180924/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beacon/probe response frame. **CVE ID: CVE-2024-33048**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ5-180924/842
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ5-180924/843
Product: ipq6000					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ6-180924/844
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation	https://docs.qualcomm.com/product/publicresources/security	H-QUA-IPQ6-180924/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ6-180924/846
Product: ipq6010					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ6-180924/847
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ6-180924/848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ6-180924/849
Product: ipq6018					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ6-180924/850
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ6-180924/851
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ6-180924/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: ipq6028					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ6-180924/853
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ6-180924/854
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ6-180924/855
Product: ipq8064					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/856
Product: ipq8065					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/857
Product: ipq8068					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/858
Product: ipq8070a					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/859
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/860
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/861
Product: ipq8071a					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/863
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/864
Product: ipq8072a					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/865
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-IPQ8-180924/866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/867
Product: ipq8074a					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/868
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/870
Product: ipq8076					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/871
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/872
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: ipq8076a					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/874
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/875
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/876
Product: ipq8078					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/877
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/878
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/879
Product: ipq8078a					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/880

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/881
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/882
Product: ipq8173					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/883
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-IPQ8-180924/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/885
Product: ipq8174					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/886
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ8-180924/888
Product: ipq9008					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ9-180924/889
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ9-180924/890
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ9-180924/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: ipq9554					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ9-180924/892
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ9-180924/893
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ9-180924/894
Product: ipq9570					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ9-180924/895
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ9-180924/896
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ9-180924/897
Product: ipq9574					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ9-180924/898

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ9-180924/899
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ9-180924/900
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-IPQ9-180924/901
Product: mdm8215					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MDM8-180924/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mdm9215					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MDM9-180924/903
Product: mdm9250					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MDM9-180924/904
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MDM9-180924/905
Product: mdm9310					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MDM9-180924/906
Product: mdm9615					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MDM9-180924/907
Product: mdm9628					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MDM9-180924/908
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MDM9-180924/909
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MDM9-180924/910
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MDM9-180924/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MDM9-180924/912
Product: mdm9640					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MDM9-180924/913
Product: mdm9645					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MDM9-180924/914
Product: mdm9650					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MDM9-180924/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MDM9-180924/916
Product: msm8108					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MSM8-180924/917
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MSM8-180924/918
Product: msm8209					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MSM8-180924/919
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MSM8-180924/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: msm8608					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MSM8-180924/921
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MSM8-180924/922
Product: msm8909w					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MSM8-180924/923
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MSM8-180924/924
Product: msm8996au					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-MSM8-180924/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33042	ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MSM8-180924/926
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MSM8-180924/927
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-MSM8-180924/928
Product: qam8255p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/929
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/930

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/931
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/932
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/933
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/934
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/935

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/936
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/937
Product: qam8295p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/938
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/939
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QAM8-180924/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command control operations. **CVE ID: CVE-2024-33052**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/941
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/942
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/943
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/944
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QAM8-180924/945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	bulletin/september-2024-bulletin.html	
Product: qam8620p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/946
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/947
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/948
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/949

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/950
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/951
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/952
Product: qam8650p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/953
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and	https://docs.qualcomm.com/product/publicres	H-QUA-QAM8-180924/954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/955
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/956
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/957
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/958

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/959
Product: qam8775p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/960
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/961
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/962
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/963

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
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/964
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/965
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/966
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAM8-180924/967
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QAM8-180924/968

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
			information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: qamsrv1h					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAMS-180924/969
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAMS-180924/970
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAMS-180924/971
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAMS-180924/972

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAMS-180924/973
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAMS-180924/974
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAMS-180924/975
Product: qamsrv1m					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAMS-180924/976
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and	https://docs.qualcomm.com/product/publicres	H-QUA-QAMS-180924/977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAMS-180924/978
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAMS-180924/979
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAMS-180924/980
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAMS-180924/981

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QAMS-180924/982
Product: qca0000					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA0-180924/983
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA0-180924/984
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA0-180924/985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: qca1062					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA1-180924/986
Product: qca1064					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA1-180924/987
Product: qca2062					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA2-180924/988
Product: qca2064					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCA2-180924/989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33051	ber-2024-bulletin.html	
Product: qca2065					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA2-180924/990
Product: qca2066					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA2-180924/991
Product: qca4024					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA4-180924/992
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA4-180924/993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA4-180924/994
Product: qca6174					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/995
Product: qca6174a					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/996
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCA6-180924/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33060	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/998
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/999
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1000
Product: qca6175a					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1002
Product: qca6310					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1003
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1004
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1005
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1007
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1008
Product: qca6320					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1009
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1010
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1012
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1013
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1014
Product: qca6335					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1015
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1017
Product: qca6391					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1018
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1019
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1020
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1021
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/pr	H-QUA-QCA6-180924/1022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1023
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1024
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1025
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1026

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
			CVE ID: CVE-2024-33057		
Product: qca6420					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1027
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1028
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1029
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1030
Product: qca6421					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCA6-180924/1031

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
			CVE ID: CVE-2024-33042	ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1032
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1033
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1034
Product: qca6426					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1035
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCA6-180924/1036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33052	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1037
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1038
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1039
Product: qca6430					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1040
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCA6-180924/1041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33052	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1042
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1043
Product: qca6431					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1044
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1045
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1047
Product: qca6436					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1048
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1049
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1050
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1051

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1052
Product: qca6554a					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1053
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1054
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1056
Product: qca6564					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1057
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1058
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1059
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCA6-180924/1060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33051	ber-2024-bulletin.html	
Product: qca6564a					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1061
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1062
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1063
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1064
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1066
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1067
Product: qca6564au					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1068
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1069
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1070

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
			CVE ID: CVE-2024-33052		
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1071
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1072
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1073
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1074
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCA6-180924/1075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1076
Product: qca6574					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1077
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1078
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1079
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	H-QUA-QCA6-180924/1080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1081
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1082
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1083
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1084

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1085
Product: qca6574a					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1086
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1087
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1088
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1089

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
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1090
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1091
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1092
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1093
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCA6-180924/1094

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
			CVE ID: CVE-2024-33051	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1095
Product: qca6574au					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1096
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1097
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1098
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCA6-180924/1099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1100
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1101
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1102
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1103
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element	https://docs.qualcomm.com/product/publicres	H-QUA-QCA6-180924/1104

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
			Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ources/security bulletin/september-2024-bulletin.html	
Product: qca6584					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1105
Product: qca6584au					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1106
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1107
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCA6-180924/1108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38401	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1109
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1110
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1111
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1112
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCA6-180924/1113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: qca6595					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1114
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1115
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1116
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1117
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	H-QUA-QCA6-180924/1118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1119
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1120
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1121
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1122

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
			CVE ID: CVE-2024-33057		
Product: qca6595au					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1123
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1124
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1125
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1126
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1127

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
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1128
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1129
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1130
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1131
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: qca6678aq					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1133
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1134
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1135
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1136
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during	https://docs.qualcomm.com/product/publicres	H-QUA-QCA6-180924/1137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1138
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1139
Product: qca6688aq					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1140
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCA6-180924/1141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1142
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1143
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1144
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1145
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element	https://docs.qualcomm.com/product/publicres	H-QUA-QCA6-180924/1146

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
			Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ources/security bulletin/september-2024-bulletin.html	
Product: qca6696					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1147
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1148
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1149
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1151
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1152
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1153
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1154
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1155

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1156
Product: qca6698aq					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1157
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1158
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1159
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1160

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
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1161
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1162
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1163
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1164
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCA6-180924/1165

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
			CVE ID: CVE-2024-33051	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1166
Product: qca6777aq					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1167
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1168
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCA6-180924/1169

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
			check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: qca6787aq					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1170
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1171
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1172
Product: qca6797aq					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1173
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1174
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1175
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1176
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1177

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1178
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA6-180924/1179
Product: qca7500					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA7-180924/1180
Product: qca8075					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCA8-180924/1181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beacon/probe response frame. **CVE ID: CVE-2024-33048**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1182
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1183
Product: qca8081					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1184
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCA8-180924/1185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1186
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1187
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1188
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1189
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicres	H-QUA-QCA8-180924/1190

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1191
Product: qca8082					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1192
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1193
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCA8-180924/1194

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
			common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	bulletin/september-2024-bulletin.html	
Product: qca8084					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1195
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1196
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca8085					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1198
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1199
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1200
Product: qca8337					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCA8-180924/1201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33045	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1202
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1203
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1204
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1205
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1206

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
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1207
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1208
Product: qca8386					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1209
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA8-180924/1211
Product: qca9367					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1212
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1213
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCA9-180924/1214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33051	ber-2024-bulletin.html	
Product: qca9377					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1215
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1216
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1217
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1218
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicres	H-QUA-QCA9-180924/1219

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	ources/security bulletin/september-2024-bulletin.html	
Product: qca9378					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1220
Product: qca9379					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1221
Product: qca9880					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1222
Product: qca9886					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1223
Product: qca9888					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1224
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1225
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: qca9889					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1227
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1228
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1229
Product: qca9898					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1230
Product: qca9980					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1231
Product: qca9984					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1232
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicres	H-QUA-QCA9-180924/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	ources/security bulletin/september-2024-bulletin.html	
Product: qca9985					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1234
Product: qca9990					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1235
Product: qca9992					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1236

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
			either missing or improper. **CVE ID: CVE-2024-33050**		
Product: qca9994					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCA9-180924/1237
Product: qcc2073					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCC2-180924/1238
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCC2-180924/1239

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCC2-180924/1240
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCC2-180924/1241
Product: qcc2076					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCC2-180924/1242
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCC2-180924/1243

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCC2-180924/1244
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCC2-180924/1245
Product: qcc710					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCC7-180924/1246
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCC7-180924/1247
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCC7-180924/1248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38402	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCC7-180924/1249
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCC7-180924/1250
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCC7-180924/1251
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCC7-180924/1252
Product: qcf8000					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCF8-180924/1253
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCF8-180924/1254
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCF8-180924/1255
Product: qcf8001					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCF8-180924/1256

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCF8-180924/1257
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCF8-180924/1258
Product: qcm2150					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM2-180924/1259
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM2-180924/1260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM2-180924/1261
Product: qcm2290					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM2-180924/1262
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM2-180924/1263
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM2-180924/1264
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM2-180924/1265
Product: qcm4290					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1266
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1267
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1268
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1269
Product: qcm4325					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1271
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1272
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1273
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1274
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1276
Product: qcm4490					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1277
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1278
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1279
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1280
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and	https://docs.qualcomm.com/product/publicres	H-QUA-QCM4-180924/1281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1282
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1283
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM4-180924/1284
Product: qcm5430					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM5-180924/1285

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM5-180924/1286
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM5-180924/1287
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM5-180924/1288
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM5-180924/1289
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM5-180924/1290
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	H-QUA-QCM5-180924/1291

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
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM5-180924/1292
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM5-180924/1293
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM5-180924/1294
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM5-180924/1295

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM5-180924/1296
Product: qcm6125					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM6-180924/1297
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM6-180924/1298
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM6-180924/1299
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM6-180924/1300

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
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM6-180924/1301
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM6-180924/1302
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM6-180924/1303
Product: qcm6490					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM6-180924/1304
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCM6-180924/1305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33042	bulletin/september-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM6-180924/1306
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM6-180924/1307
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM6-180924/1308
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM6-180924/1309
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCM6-180924/1310

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
			CVE ID: CVE-2024-33060	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM6-180924/1311
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM6-180924/1312
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM6-180924/1313
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM6-180924/1314
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCM6-180924/1315

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
			information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: qcm8550					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM8-180924/1316
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM8-180924/1317
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM8-180924/1318
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM8-180924/1319
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCM8-180924/1320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM8-180924/1321
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM8-180924/1322
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM8-180924/1323
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM8-180924/1324

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM8-180924/1325
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCM8-180924/1326
Product: qcn5022					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1327
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1329
Product: qcn5024					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1330
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1331
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: qcn5052					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1333
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1334
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1335
Product: qcn5122					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1336
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1337
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1338
Product: qcn5124					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1340
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1341
Product: qcn5152					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1342
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCN5-180924/1343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1344
Product: qcn5154					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1345
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1347
Product: qcn5164					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1348
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1349
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN5-180924/1350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: qcn6023					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1351
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1352
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1353
Product: qcn6024					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1354
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1355
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1356
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1357
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1358

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1359
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1360
Product: qcn6112					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1361
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1363
Product: qcn6122					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1364
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1365
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCN6-180924/1366

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
			check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: qcn6132					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1367
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1368
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1369
Product: qcn6224					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1370
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1371
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1372
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1373
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1374

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1375
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1376
Product: qcn6274					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1377
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1378
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	H-QUA-QCN6-180924/1379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1380
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1381
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1382
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1383

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
			CVE ID: CVE-2024-33057		
Product: qcn6402					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1384
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1385
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1386
Product: qcn6412					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-	https://docs.qualcomm.com/product/publicres	H-QUA-QCN6-180924/1387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1388
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1389
Product: qcn6422					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1391
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1392
Product: qcn6432					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1393
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN6-180924/1395
Product: qcn7605					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN7-180924/1396
Product: qcn7606					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN7-180924/1397
Product: qcn9000					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCN9-180924/1398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1399
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1400
Product: qcn9011					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1401
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCN9-180924/1402

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
			node simultaneously. **CVE ID: CVE-2024-33060**	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1403
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1404
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1405
Product: qcn9012					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1406
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	H-QUA-QCN9-180924/1407

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
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1408
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1409
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1410
Product: qcn9022					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1411

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1412
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1413
Product: qcn9024					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1414
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1415

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
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1416
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1417
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1418
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1419
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCN9-180924/1420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: qcn9070					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1421
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1422
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1423
Product: qcn9072					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1424
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1425
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1426
Product: qcn9074					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1427

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
			CVE ID: CVE-2024-33060		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1428
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1429
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1430
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1431
Product: qcn9100					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1432
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1433
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1434
Product: qcn9160					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1435

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1436
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1437
Product: qcn9274					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1438
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1440
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCN9-180924/1441
Product: qcs2290					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS2-180924/1442
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS2-180924/1443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS2-180924/1444
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS2-180924/1445
Product: qcs410					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1446
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1447
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1448
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	H-QUA-QCS4-180924/1449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1450
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1451
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1452
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1453
Product: qcs4290					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1454
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1455
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1456
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1457
Product: qcs4490					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1458

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1459
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1460
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1461
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1462
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1463
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCS4-180924/1464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS4-180924/1465
Product: qcs5430					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS5-180924/1466
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS5-180924/1467
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS5-180924/1468
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCS5-180924/1469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invoked from user-space. **CVE ID: CVE-2024-33047**	bulletin/september-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS5-180924/1470
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS5-180924/1471
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS5-180924/1472
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS5-180924/1473
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCS5-180924/1474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beacon/probe response frame. **CVE ID: CVE-2024-33048**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS5-180924/1475
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS5-180924/1476
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS5-180924/1477
Product: qcs610					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCS6-180924/1478

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
			CVE ID: CVE-2024-33042	ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1479
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1480
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1481
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1482
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1483
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during	https://docs.qualcomm.com/product/publicres	H-QUA-QCS6-180924/1484

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
			new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1485
Product: qcs6125					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1486
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1487
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1488
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	H-QUA-QCS6-180924/1489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1490
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1491
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1492
Product: qcs6490					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1493

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1494
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1495
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1496
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1497
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1498
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	H-QUA-QCS6-180924/1499

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
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1500
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1501
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1502
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1503

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS6-180924/1504
Product: qcs7230					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS7-180924/1505
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS7-180924/1506
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS7-180924/1507
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS7-180924/1508

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
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS7-180924/1509
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS7-180924/1510
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS7-180924/1511
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS7-180924/1512
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QCS7-180924/1513

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
			information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: qcs8250					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1514
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1515
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1516
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1517
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	H-QUA-QCS8-180924/1518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1519
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1520
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1521
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1522

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
			CVE ID: CVE-2024-33057		
Product: qcs8550					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1523
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1524
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1525
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1526
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33054		
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1528
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1529
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1530
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1531
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCS8-180924/1532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QCS8-180924/1533
Product: qdu1000					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDU1-180924/1534
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDU1-180924/1535
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDU1-180924/1536
Product: qdu1010					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDU1-180924/1537
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDU1-180924/1538
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDU1-180924/1539
Product: qdu1110					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDU1-180924/1540
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDU1-180924/1541

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
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDU1-180924/1542
Product: qdu1210					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDU1-180924/1543
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDU1-180924/1544
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDU1-180924/1545
Product: qdx1010					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDX1-180924/1546

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
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDX1-180924/1547
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDX1-180924/1548
Product: qdx1011					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDX1-180924/1549
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDX1-180924/1550
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QDX1-180924/1551
Product: qep8111					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QEP8-180924/1552
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QEP8-180924/1553
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QEP8-180924/1554
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QEP8-180924/1555
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QEP8-180924/1556

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
Product: qfw7114					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QFW7-180924/1557
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QFW7-180924/1558
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QFW7-180924/1559
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QFW7-180924/1560
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QFW7-180924/1561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QFW7-180924/1562
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QFW7-180924/1563
Product: qfw7124					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QFW7-180924/1564
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QFW7-180924/1565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QFW7-180924/1566
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QFW7-180924/1567
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QFW7-180924/1568
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QFW7-180924/1569
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QFW7-180924/1570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: qrb5165m					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRB5-180924/1571
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRB5-180924/1572
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRB5-180924/1573
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRB5-180924/1574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRB5-180924/1575
Product: qrb5165n					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRB5-180924/1576
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRB5-180924/1577
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRB5-180924/1578
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRB5-180924/1579

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRB5-180924/1580
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRB5-180924/1581
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRB5-180924/1582
Product: qru1032					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRU1-180924/1583
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and	https://docs.qualcomm.com/product/publicres	H-QUA-QRU1-180924/1584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRU1-180924/1585
Product: qru1052					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRU1-180924/1586
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRU1-180924/1587
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRU1-180924/1588
Product: qru1062					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRU1-180924/1589
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRU1-180924/1590
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QRU1-180924/1591
Product: qsm8250					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QSM8-180924/1592
Product: qsm8350					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QSM8-180924/1593

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
			CVE ID: CVE-2024-33045		
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QSM8-180924/1594
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QSM8-180924/1595
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QSM8-180924/1596
Product: qxm8083					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QXM8-180924/1597
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-QXM8-180924/1598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-QXM8-180924/1599
Product: robotics_rb3					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-ROBO-180924/1600
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-ROBO-180924/1601
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-ROBO-180924/1602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: robotics_rb5					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-ROBO-180924/1603
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-ROBO-180924/1604
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-ROBO-180924/1605
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-ROBO-180924/1606
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-ROBO-180924/1607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-ROBO-180924/1608
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-ROBO-180924/1609
Product: sa4150p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA41-180924/1610
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA41-180924/1611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA41-180924/1612
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA41-180924/1613
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA41-180924/1614
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA41-180924/1615
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA41-180924/1616
Product: sa4155p					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA41-180924/1617
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA41-180924/1618
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA41-180924/1619
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA41-180924/1620
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA41-180924/1621
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SA41-180924/1622

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
			in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA41-180924/1623
Product: sa6145p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1624
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1625
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1626
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and	https://docs.qualcomm.com/product/publicres	H-QUA-SA61-180924/1627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1628
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1629
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1630
Product: sa6150p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1632
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1633
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1634
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1635
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1636

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1637
Product: sa6155					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1638
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1639
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1640
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1641
Product: sa6155p					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1642
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1643
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1644
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1645
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1646
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SA61-180924/1647

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
			element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1648
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1649
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA61-180924/1650
Product: sa7255p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SA72-180924/1651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA72-180924/1652
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA72-180924/1653
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA72-180924/1654
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA72-180924/1655

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA72-180924/1656
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA72-180924/1657
Product: sa7775p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA77-180924/1658
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA77-180924/1659
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SA77-180924/1660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38402	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA77-180924/1661
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA77-180924/1662
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA77-180924/1663
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA77-180924/1664
Product: sa8145p					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1665
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1666
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1667
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1668
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1669
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SA81-180924/1670

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
			in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1671
Product: sa8150p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1672
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1673
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1674
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and	https://docs.qualcomm.com/product/publicres	H-QUA-SA81-180924/1675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1676
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1677
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1678
Product: sa8155					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1680
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1681
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1682
Product: sa8155p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1683
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1685
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1686
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1687
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1688
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1689

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1690
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1691
Product: sa8195p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1692
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1693
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SA81-180924/1694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command control operations. **CVE ID: CVE-2024-33052**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1695
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1696
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1697
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1698

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1699
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA81-180924/1700
Product: sa8255p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA82-180924/1701
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA82-180924/1702
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA82-180924/1703

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
			CVE ID: CVE-2024-33052		
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA82-180924/1704
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA82-180924/1705
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA82-180924/1706
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA82-180924/1707
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SA82-180924/1708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA82-180924/1709
Product: sa8295p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA82-180924/1710
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA82-180924/1711
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA82-180924/1712
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	H-QUA-SA82-180924/1713

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
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA82-180924/1714
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA82-180924/1715
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA82-180924/1716
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA82-180924/1717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33057		
Product: sa8530p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA85-180924/1718
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA85-180924/1719
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA85-180924/1720
Product: sa8540p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SA85-180924/1721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33045	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA85-180924/1722
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA85-180924/1723
Product: sa8620p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA86-180924/1724
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA86-180924/1725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA86-180924/1726
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA86-180924/1727
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA86-180924/1728
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA86-180924/1729
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SA86-180924/1730

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
			information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: sa8650p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA86-180924/1731
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA86-180924/1732
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA86-180924/1733
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA86-180924/1734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA86-180924/1735
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA86-180924/1736
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA86-180924/1737
Product: sa8770p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA87-180924/1738
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new	https://docs.qualcomm.com/product/publicres	H-QUA-SA87-180924/1739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA87-180924/1740
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA87-180924/1741
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA87-180924/1742
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA87-180924/1743
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SA87-180924/1744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA87-180924/1745
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA87-180924/1746
Product: sa8775p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA87-180924/1747
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA87-180924/1748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA87-180924/1749
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA87-180924/1750
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA87-180924/1751
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA87-180924/1752
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA87-180924/1753

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA87-180924/1754
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA87-180924/1755
Product: sa9000p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA90-180924/1756
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA90-180924/1757
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SA90-180924/1758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command control operations. **CVE ID: CVE-2024-33052**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA90-180924/1759
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA90-180924/1760
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA90-180924/1761
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA90-180924/1762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA90-180924/1763
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SA90-180924/1764
Product: sc8180x					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SC81-180924/1765
Product: sc8380xp					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SC83-180924/1766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SC83-180924/1767
Product: sd460					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD46-180924/1768
Product: sd626					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD62-180924/1769
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD62-180924/1770
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD62-180924/1771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33060		
Product: sd660					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD66-180924/1772
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD66-180924/1773
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD66-180924/1774
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD66-180924/1775
Product: sd662					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SD66-180924/1776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	ber-2024-bulletin.html	
Product: sd670					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD67-180924/1777
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD67-180924/1778
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD67-180924/1779
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD67-180924/1780
Product: sd675					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD67-180924/1781
Product: sd730					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD73-180924/1782
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD73-180924/1783
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD73-180924/1784
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD73-180924/1785
Product: sd835					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD83-180924/1786
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD83-180924/1787
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD83-180924/1788
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD83-180924/1789
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD83-180924/1790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD83-180924/1791
Product: sd855					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD85-180924/1792
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD85-180924/1793
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD85-180924/1794
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD85-180924/1795
Product: sd865_5g					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD86-180924/1796
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD86-180924/1797
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD86-180924/1798
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD86-180924/1799
Product: sd888					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD88-180924/1800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD88-180924/1801
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD88-180924/1802
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD88-180924/1803
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD88-180924/1804
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD88-180924/1805

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD88-180924/1806
Product: sdm429w					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDM4-180924/1807
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDM4-180924/1808
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDM4-180924/1809
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDM4-180924/1810

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
			CVE ID: CVE-2024-33054		
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDM4-180924/1811
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDM4-180924/1812
Product: sdx20m					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDX2-180924/1813
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDX2-180924/1814
Product: sdx55					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDX5-180924/1815
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDX5-180924/1816
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDX5-180924/1817
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDX5-180924/1818
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDX5-180924/1819
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during	https://docs.qualcomm.com/product/publicres	H-QUA-SDX5-180924/1820

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
			new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDX5-180924/1821
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDX5-180924/1822
Product: sdx61					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDX6-180924/1823
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SDX6-180924/1824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDX6-180924/1825
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDX6-180924/1826
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDX6-180924/1827
Product: sdx65m					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDX6-180924/1828

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDX6-180924/1829
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SDX6-180924/1830
Product: sd_455					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD_4-180924/1831
Product: sd_675					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD_6-180924/1832

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
Product: sd_8cx					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD_8-180924/1833
Product: sd_8_gen1_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD_8-180924/1834
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD_8-180924/1835
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD_8-180924/1836
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD_8-180924/1837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD_8-180924/1838
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD_8-180924/1839
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD_8-180924/1840
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SD_8-180924/1841
Product: sg4150p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SG41-180924/1842

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
			CVE ID: CVE-2024-33042	ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SG41-180924/1843
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SG41-180924/1844
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SG41-180924/1845
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SG41-180924/1846
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SG41-180924/1847

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SG41-180924/1848
Product: sg8275p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SG82-180924/1849
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SG82-180924/1850
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SG82-180924/1851
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SG82-180924/1852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SG82-180924/1853
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SG82-180924/1854
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SG82-180924/1855
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SG82-180924/1856

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
			CVE ID: CVE-2024-33057		
Product: sm4125					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM41-180924/1857
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM41-180924/1858
Product: sm4635					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM46-180924/1859
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM46-180924/1860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sm6250					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM62-180924/1861
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM62-180924/1862
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM62-180924/1863
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM62-180924/1864
Product: sm6250p					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM62-180924/1865

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
			CVE ID: CVE-2024-33051		
Product: sm6370					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM63-180924/1866
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM63-180924/1867
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM63-180924/1868
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM63-180924/1869
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicres	H-QUA-SM63-180924/1870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	ources/security bulletin/september-2024-bulletin.html	
Product: sm7250p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM72-180924/1871
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM72-180924/1872
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM72-180924/1873
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM72-180924/1874
Product: sm7315					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM73-180924/1875
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM73-180924/1876
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM73-180924/1877
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM73-180924/1878
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM73-180924/1879
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SM73-180924/1880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM73-180924/1881
Product: sm7325p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM73-180924/1882
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM73-180924/1883
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM73-180924/1884
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SM73-180924/1885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM73-180924/1886
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM73-180924/1887
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM73-180924/1888
Product: sm7435					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM74-180924/1889

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM74-180924/1890
Product: sm8550p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM85-180924/1891
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM85-180924/1892
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM85-180924/1893
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM85-180924/1894
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake	https://docs.qualcomm.com/product/publicres	H-QUA-SM85-180924/1895

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
			between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM85-180924/1896
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM85-180924/1897
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM85-180924/1898
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM85-180924/1899

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM85-180924/1900
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM85-180924/1901
Product: sm8635					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM86-180924/1902
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM86-180924/1903
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SM86-180924/1904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	bulletin/september-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM86-180924/1905
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM86-180924/1906
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM86-180924/1907
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM86-180924/1908
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SM86-180924/1909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beacon/probe response frame. **CVE ID: CVE-2024-33048**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM86-180924/1910
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM86-180924/1911
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM86-180924/1912
Product: sm8750					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SM87-180924/1913

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
			CVE ID: CVE-2024-33042	ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SM87-180924/1914
Product: smart_audio_200					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SMAR-180924/1915
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SMAR-180924/1916
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SMAR-180924/1917
Product: smart_audio_400					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SMAR-180924/1918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33045	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SMAR-180924/1919
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SMAR-180924/1920
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SMAR-180924/1921
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SMAR-180924/1922
Product: smart_display_200					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative	https://docs.qualcomm.com/product/publicres	H-QUA-SMAR-180924/1923

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
			Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SMAR-180924/1924
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SMAR-180924/1925
Product: snapdragon_1200_wearable					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1926
Product: snapdragon_208					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1927

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1928
Product: snapdragon_210					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1929
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1930
Product: snapdragon_212					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1931
Product: snapdragon_212_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/1932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33052	ber-2024-bulletin.html	
Product: snapdragon_425					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1933
Product: snapdragon_425_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1934
Product: snapdragon_429					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1935
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1936
Product: snapdragon_429_mobile					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1937
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1938
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1939
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1940
Product: snapdragon_439					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/1941

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
			CVE ID: CVE-2024-33042	ber-2024-bulletin.html	
Product: snapdragon_439_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1942
Product: snapdragon_460					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1943
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1944
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1946
Product: snapdragon_460_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1947
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1948
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1949
Product: snapdragon_480\+_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1950

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1951
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1952
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1953
Product: snapdragon_480\+_5g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1954
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/1955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33060	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1956
Product: snapdragon_480_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1957
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1958
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1959
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/1960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	ber-2024-bulletin.html	
Product: snapdragon_480_5g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1961
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1962
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1963
Product: snapdragon_4_gen_1					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1965
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1966
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1967
Product: snapdragon_4_gen_1_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1968
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/1969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33060	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1970
Product: snapdragon_4_gen_2					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1971
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1972
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1973
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1975
Product: snapdragon_4_gen_2_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1976
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1977
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1978
Product: snapdragon_625					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1979
Product: snapdragon_625_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1980
Product: snapdragon_626					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1981
Product: snapdragon_626_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1982
Product: snapdragon_630					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-180924/1983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1984
Product: snapdragon_630_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1985
Product: snapdragon_632					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1986
Product: snapdragon_632_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1987

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
Product: snapdragon_636					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1988
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1989
Product: snapdragon_636_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1990
Product: snapdragon_660					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1991
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/1992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33051	ber-2024-bulletin.html	
Product: snapdragon_660_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1993
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1994
Product: snapdragon_662					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1995
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1996
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/1997

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
			frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1998
Product: snapdragon_662_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/1999
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2000
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2001
Product: snapdragon_665					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2002
Product: snapdragon_670					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2003
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2004
Product: snapdragon_670_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2005
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2006

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
			CVE ID: CVE-2024-33060		
Product: snapdragon_675					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2007
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2008
Product: snapdragon_675_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2009
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2010
Product: snapdragon_678					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2011
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2012
Product: snapdragon_678_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2013
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2014
Product: snapdragon_680_4g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2015

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2016
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2017
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2018
Product: snapdragon_680_4g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2019
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/2020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33060	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2021
Product: snapdragon_685_4g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2022
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2023
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2024
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/2025

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	ber-2024-bulletin.html	
Product: snapdragon_685_4g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2026
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2027
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2028
Product: snapdragon_690_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2030
Product: snapdragon_690_5g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2031
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2032
Product: snapdragon_695_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2033
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2034

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
			CVE ID: CVE-2024-33045		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2035
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2036
Product: snapdragon_695_5g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2037
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2038
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-180924/2039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	ources/security bulletin/september-2024-bulletin.html	
Product: snapdragon_6_gen_1					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2040
Product: snapdragon_6_gen_1_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2041
Product: snapdragon_710					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2042
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2043
Product: snapdragon_710_mobile					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2044
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2045
Product: snapdragon_712					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2046
Product: snapdragon_720g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2047
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/2048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33051	ber-2024-bulletin.html	
Product: snapdragon_720g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2049
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2050
Product: snapdragon_730					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2051
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2052
Product: snapdragon_730g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2053
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2054
Product: snapdragon_730g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2055
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2056
Product: snapdragon_730_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2057

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
			CVE ID: CVE-2024-33052		
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2058
Product: snapdragon_732g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2059
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2060
Product: snapdragon_732g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2061
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/2062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	ber-2024-bulletin.html	
Product: snapdragon_750g_5g					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2063
Product: snapdragon_750g_5g_mobile					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2064
Product: snapdragon_765g_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2065
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2066

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
Product: snapdragon_765g_5g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2067
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2068
Product: snapdragon_765_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2069
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2070
Product: snapdragon_765_5g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-180924/2071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command control operations. **CVE ID: CVE-2024-33052**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2072
Product: snapdragon_768g_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2073
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2074
Product: snapdragon_768g_5g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2075
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	H-QUA-SNAP-180924/2076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Product: snapdragon_778g\+_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2077
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2078
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2079
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_778g\+_5g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2081
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2082
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2083
Product: snapdragon_778g_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2084
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2086
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2087
Product: snapdragon_778g_5g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2088
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2089
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/2090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38402	ber-2024-bulletin.html	
Product: snapdragon_780g_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2091
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2092
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2093
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2094
Product: snapdragon_780g_5g_mobile					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2095
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2096
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2097
Product: snapdragon_782g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2098
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2100
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2101
Product: snapdragon_782g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2102
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2103
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/2104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38402	ber-2024-bulletin.html	
Product: snapdragon_7c\+_gen_3					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2105
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2106
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2107
Product: snapdragon_7c\+_gen_3_compute					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2109
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2110
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2111
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2112
Product: snapdragon_7c_compute					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2113
Product: snapdragon_7c_gen_2_compute					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2114
Product: snapdragon_7\+_gen_2					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2115
Product: snapdragon_7\+_gen_2_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2116
Product: snapdragon_7_gen_1					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2117
Product: snapdragon_7_gen_1_mobile					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2118
Product: snapdragon_820_automotive					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2119
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2120
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2121
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2122
Product: snapdragon_835_mobile_pc					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2123
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2124
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2125
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2126
Product: snapdragon_835_pc					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/2127

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
			CVE ID: CVE-2024-33045	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2128
Product: snapdragon_845					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2129
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2130
Product: snapdragon_845_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2131
Product: snapdragon_850_compute					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-180924/2132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	ources/security bulletin/september-2024-bulletin.html	
Product: snapdragon_855					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2133
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2134
Product: snapdragon_855\+					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2135
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2136
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-180924/2137

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	bulletin/september-2024-bulletin.html	
Product: snapdragon_855\+_mobile					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2138
Product: snapdragon_855_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2139
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2140
Product: snapdragon_860					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/2141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33042	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2142
Product: snapdragon_860_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2143
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2144
Product: snapdragon_865\+_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2145
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/2146

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	ber-2024-bulletin.html	
Product: snapdragon_865\+_5g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2147
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2148
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2149
Product: snapdragon_865_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2151
Product: snapdragon_865_5g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2152
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2153
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2154
Product: snapdragon_870_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/2155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33042	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2156
Product: snapdragon_870_5g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2157
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2158
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2159
Product: snapdragon_888\+_5g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2160
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2161
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2162
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2163
Product: snapdragon_888\+_5g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2164

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
			CVE ID: CVE-2024-33052		
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2165
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2166
Product: snapdragon_888_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2167
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2168
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2170
Product: snapdragon_888_5g_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2171
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2172
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2173
Product: snapdragon_8cx_compute					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2174
Product: snapdragon_8cx_gen_2_5g_compute					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2175
Product: snapdragon_8cx_gen_3					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2176
Product: snapdragon_8cx_gen_3_compute					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2177
Product: snapdragon_8c_compute					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2178
Product: snapdragon_8\+_gen_1					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2179
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2180
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2181
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2183
Product: snapdragon_8\+_gen_1_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2184
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2185
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2186
Product: snapdragon_8\+_gen_2					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupt	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/2187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ed pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2188
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2189
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2190
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2191
Product: snapdragon_8\+_gen_2_mobile					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2192
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2193
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2194
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2195
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2196

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2197
Product: snapdragon_8_gen_1					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2198
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2199
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2200
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2201

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
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2202
Product: snapdragon_8_gen_1_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2203
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2204
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2205
Product: snapdragon_8_gen_2					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2206
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2207
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2208
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2209
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2210
Product: snapdragon_8_gen_2_mobile					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2211
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2212
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2213
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2214
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2216
Product: snapdragon_8_gen_3					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2217
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2218
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2219
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-180924/2220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2221
Product: snapdragon_8_gen_3_mobile					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2222
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2223
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2225
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2226
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2227
Product: snapdragon_ar2_gen_1					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2228

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2229
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2230
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2231
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2232
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2233

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2234
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2235
Product: snapdragon_auto_4g					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2236
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2237
Product: snapdragon_auto_5g-rf					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2238
Product: snapdragon_auto_5g-rf_gen_2					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2239
Product: snapdragon_auto_5g_modem-rf					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2240
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2241
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/2242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2243
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2244
Product: snapdragon_auto_5g_modem-rf_gen_2					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2245
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2246
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-180924/2247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2248
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2249
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2250
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2251

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
			CVE ID: CVE-2024-33057		
Product: snapdragon_w5\+_gen_1					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2252
Product: snapdragon_w5\+_gen_1_wearable					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2253
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2254
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2255
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/2256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2257
Product: snapdragon_wear_2100					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2258
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2259
Product: snapdragon_wear_2500					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2261
Product: snapdragon_wear_3100					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2262
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2263
Product: snapdragon_x12_lte					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2264
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2265

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
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2266
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2267
Product: snapdragon_x20_lte					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2268
Product: snapdragon_x35_5g-rf_system					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2269
Product: snapdragon_x35_5g_modem-rf					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/pr	H-QUA-SNAP-180924/2270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Product: snapdragon_x35_5g_modem-rf_system					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2271
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2272
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2273
Product: snapdragon_x50_5g-rf_system					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/2274

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
			CVE ID: CVE-2024-33051	ber-2024-bulletin.html	
Product: snapdragon_x50_5g_modem-rf_system					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2275
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2276
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2277
Product: snapdragon_x55_5g-rf_system					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2278
Product: snapdragon_x55_5g_modem-rf_system					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2279
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2280
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2281
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2282
Product: snapdragon_x5_lte					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2283

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
Product: snapdragon_x62_5g-rf_system					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2284
Product: snapdragon_x62_5g_modem-rf					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2285
Product: snapdragon_x62_5g_modem-rf_system					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2286
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2287
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-180924/2288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	bulletin/september-2024-bulletin.html	
Product: snapdragon_x65_5g-rf_system					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2289
Product: snapdragon_x65_5g_modem-rf					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2290
Product: snapdragon_x65_5g_modem-rf_system					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2291
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SNAP-180924/2292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2293
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2294
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2295
Product: snapdragon_x72_5g-rf_system					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-180924/2296

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	bulletin/september-2024-bulletin.html	
Product: snapdragon_x72_5g_modem-rf					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2297
Product: snapdragon_x72_5g_modem-rf_system					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2298
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2299
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2301
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2302
Product: snapdragon_x75_5g-rf_system					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2303
Product: snapdragon_x75_5g_modem-rf					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_x75_5g_modem-rf_system					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2305
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2306
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2307
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2308
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-180924/2309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	bulletin/september-2024-bulletin.html	
Product: snapdragon_xr1					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2310
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2311
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2312
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2313
Product: snapdragon_xr2\+_gen_1					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2314
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2315
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2316
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2317
Product: snapdragon_xr2_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2319
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2320
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SNAP-180924/2321
Product: srv1h					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2322
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2323

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
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2324
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2325
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2326
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2327
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: srv1l					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2329
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2330
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2331
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2332
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during	https://docs.qualcomm.com/product/publicres	H-QUA-SRV1-180924/2333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2334
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2335
Product: srv1m					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2336
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SRV1-180924/2337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2338
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2339
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2340
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SRV1-180924/2341
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element	https://docs.qualcomm.com/product/publicres	H-QUA-SRV1-180924/2342

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
			Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ources/security bulletin/september-2024-bulletin.html	
Product: ssg2115p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SSG2-180924/2343
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SSG2-180924/2344
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SSG2-180924/2345
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SSG2-180924/2346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SSG2-180924/2347
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SSG2-180924/2348
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SSG2-180924/2349
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SSG2-180924/2350
Product: ssg2125p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SSG2-180924/2351
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SSG2-180924/2352
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SSG2-180924/2353
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SSG2-180924/2354
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SSG2-180924/2355
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during	https://docs.qualcomm.com/product/publicres	H-QUA-SSG2-180924/2356

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
			new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SSG2-180924/2357
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SSG2-180924/2358
Product: sw5100					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SW51-180924/2359
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SW51-180924/2360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SW51-180924/2361
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SW51-180924/2362
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SW51-180924/2363
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SW51-180924/2364
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicres	H-QUA-SW51-180924/2365

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	ources/security bulletin/september-2024-bulletin.html	
Product: sw5100p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SW51-180924/2366
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SW51-180924/2367
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SW51-180924/2368
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SW51-180924/2369
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SW51-180924/2370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beacon/probe response frame. **CVE ID: CVE-2024-33048**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SW51-180924/2371
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SW51-180924/2372
Product: sxr1120					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR1-180924/2373
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR1-180924/2374
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	H-QUA-SXR1-180924/2375

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
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR1-180924/2376
Product: sxr1230p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR1-180924/2377
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR1-180924/2378
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR1-180924/2379
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	H-QUA-SXR1-180924/2380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/security bulletin/september-2024-bulletin.html	H-QUA-SXR1-180924/2381
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/security bulletin/september-2024-bulletin.html	H-QUA-SXR1-180924/2382
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/security bulletin/september-2024-bulletin.html	H-QUA-SXR1-180924/2383
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	https://docs.qualcomm.com/product/publicresources/security bulletin/september-2024-bulletin.html	H-QUA-SXR1-180924/2384

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
			CVE ID: CVE-2024-33057		
Product: sxr2130					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2385
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2386
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2387
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2388
Product: sxr2230p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SXR2-180924/2389

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
			CVE ID: CVE-2024-33042	ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2390
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2391
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2392
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2393
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2394

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2395
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2396
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2397
Product: sxr2250p					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2398
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new	https://docs.qualcomm.com/product/publicres	H-QUA-SXR2-180924/2399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2400
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2401
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2402
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2403
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-SXR2-180924/2404

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
			length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2405
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-SXR2-180924/2406
Product: talynplus					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-TALY-180924/2407
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-TALY-180924/2408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-TALY-180924/2409
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-TALY-180924/2410
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-TALY-180924/2411
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-TALY-180924/2412
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-TALY-180924/2413
Product: video_collaboration_vc1					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2414
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2415
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2416
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2417
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2418
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-VIDE-180924/2419

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
			CVE ID: CVE-2024-38402	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2420
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2421
Product: video_collaboration_vc3					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2422
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2423
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new	https://docs.qualcomm.com/product/publicres	H-QUA-VIDE-180924/2424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2425
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2426
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2427
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2428
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicresources/security	H-QUA-VIDE-180924/2429

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
			concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2430
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2431
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2432
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2433
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element	https://docs.qualcomm.com/product/publicres	H-QUA-VIDE-180924/2434

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
			Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ources/security bulletin/september-2024-bulletin.html	
Product: video_collaboration_vc5					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2435
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2436
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2437
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2439
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2440
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2441
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2442
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VIDE-180924/2443

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
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: vision_intelligence_100					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VISI-180924/2444
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VISI-180924/2445
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VISI-180924/2446
Product: vision_intelligence_200					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VISI-180924/2447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VISI-180924/2448
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VISI-180924/2449
Product: vision_intelligence_300					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VISI-180924/2450
Product: vision_intelligence_400					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VISI-180924/2451
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VISI-180924/2452

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
			CVE ID: CVE-2024-33045		
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VISI-180924/2453
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VISI-180924/2454
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VISI-180924/2455
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-VISI-180924/2456
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-VISI-180924/2457

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
			check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: wcd9326					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2458
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2459
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2460
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2461
Product: wcd9330					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2462
Product: wcd9335					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2463
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2464
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2465
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2466
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/pr	H-QUA-WCD9-180924/2467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2468
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2469
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2470
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2471

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
			CVE ID: CVE-2024-33057		
Product: wcd9340					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2472
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2473
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2474
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2475
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2477
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2478
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2479
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2480
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: wcd9341					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2482
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2483
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2484
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2485
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-WCD9-180924/2486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38401	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2487
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2488
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2489
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2490
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-WCD9-180924/2491

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
			information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: wcd9360					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2492
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2493
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2494
Product: wcd9370					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2496
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2497
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2498
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2499
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2500
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	H-QUA-WCD9-180924/2501

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
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2502
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2503
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2504
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2505

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2506
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2507
Product: wcd9371					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2508
Product: wcd9375					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2509
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCD9-180924/2510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	bulletin/september-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2511
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2512
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2513
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2514
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	H-QUA-WCD9-180924/2515

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
			node simultaneously. **CVE ID: CVE-2024-33060**	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2516
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2517
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2518
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2519
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element	https://docs.qualcomm.com/product/publicres	H-QUA-WCD9-180924/2520

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
			Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ources/security bulletin/september-2024-bulletin.html	
Product: wcd9378					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2521
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2522
Product: wcd9380					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2523

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2524
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2525
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2526
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2527
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2528
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	H-QUA-WCD9-180924/2529

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
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2530
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2531
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2532
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2533

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2534
Product: wcd9385					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2535
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2536
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2537
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2538

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
			CVE ID: CVE-2024-33047		
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2539
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2540
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2541
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2542
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2543

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2544
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2545
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2546
Product: wcd9390					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2547

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2548
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2549
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2550
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2551
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2552
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/pr	H-QUA-WCD9-180924/2553

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
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2554
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2555
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2556
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2557

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
			CVE ID: CVE-2024-33057		
Product: wcd9395					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2558
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2559
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2560
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2561
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33054		
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2563
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2564
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2565
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2566
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCD9-180924/2567

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCD9-180924/2568
Product: wcn3610					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2569
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2570
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2571
Product: wcn3615					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2572
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2573
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2574
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2575
Product: wcn3620					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2577
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2578
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2579
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2580
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2581

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
			CVE ID: CVE-2024-33048		
Product: wcn3660b					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2582
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2583
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2584
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2585
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCN3-180924/2586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2587
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2588
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2589
Product: wcn3680					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2590
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCN3-180924/2591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command control operations. **CVE ID: CVE-2024-33052**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2592
Product: wcn3680b					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2593
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2594
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2595
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCN3-180924/2596

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
			CVE ID: CVE-2024-38401	bulletin/september-2024-bulletin.html	
Product: wcn3910					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2597
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2598
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2599
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2600
Product: wcn3950					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupt	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCN3-180924/2601

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
			ed pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	bulletin/september-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2602
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2603
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2604
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2605
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2606

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
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2607
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2608
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2609
Product: wcn3980					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2610
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2611

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2612
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2613
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2614
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2615
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2616
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during	https://docs.qualcomm.com/product/publicres	H-QUA-WCN3-180924/2617

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
			new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2618
Product: wcn3988					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2619
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2620
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2622
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2623
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2624
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2625
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2626
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during	https://docs.qualcomm.com/product/publicres	H-QUA-WCN3-180924/2627

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
			new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2628
Product: wcn3990					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2629
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2630
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2631
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	H-QUA-WCN3-180924/2632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2633
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2634
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2635
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2636

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
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: wcn3999					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN3-180924/2637
Product: wcn6740					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN6-180924/2638
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN6-180924/2639
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN6-180924/2640
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI	https://docs.qualcomm.com/product/publicres	H-QUA-WCN6-180924/2641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command control operations. **CVE ID: CVE-2024-33052**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN6-180924/2642
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN6-180924/2643
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN6-180924/2644
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN6-180924/2645
Product: wcn6755					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN6-180924/2646
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN6-180924/2647
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN6-180924/2648
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN6-180924/2649
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN6-180924/2650
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and	https://docs.qualcomm.com/product/publicres	H-QUA-WCN6-180924/2651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN6-180924/2652
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN6-180924/2653
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN6-180924/2654
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN6-180924/2655

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN6-180924/2656
Product: wcn7880					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WCN7-180924/2657
Product: wsa8810					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2658
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2659
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WSA8-180924/2660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	bulletin/september-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2661
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2662
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2663
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2664
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2665

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2666
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2667
Product: wsa8815					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2668
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2669
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WSA8-180924/2670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	bulletin/september-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2671
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2672
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2673
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2674
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2675

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2676
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2677
Product: wsa8830					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2678
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2679
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WSA8-180924/2680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2681
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2682
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2683
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2684
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WSA8-180924/2685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2686
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2687
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2688
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2689
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element	https://docs.qualcomm.com/product/publicres	H-QUA-WSA8-180924/2690

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
			Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ources/security bulletin/september-2024-bulletin.html	
Product: wsa8832					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2691
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2692
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2693
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2695
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2696
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2697
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2698
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2700
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2701
Product: wsa8835					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2702
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2704
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2705
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2706
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2707
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2709
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2710
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2711
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2712
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2713

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2714
Product: wsa8840					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2715
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2716
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2717
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2718

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
			CVE ID: CVE-2024-33047		
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2719
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2720
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2721
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2722
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2723

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2724
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2725
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2726
Product: wsa8845					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2727

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2728
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2729
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2730
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2731
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2732
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	H-QUA-WSA8-180924/2733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2734
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2735
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2736
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2737

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2738
Product: wsa8845h					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2739
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2740
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2741
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2742

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
			CVE ID: CVE-2024-33047		
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2743
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2744
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2745
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2746
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2747

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2748
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2749
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	H-QUA-WSA8-180924/2750
Vendor: Samsung					
Product: exynos_1080					
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280,	https://semiconductor.samsung.com/support/quality-support/produc	H-SAM-EXYN-180924/2751

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
			Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**	t-security-updates/	
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_rx_range_done_ind(), there is no input validation check on rtt_id coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27387**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27387/	H-SAM-EXYN-180924/2752
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-	H-SAM-EXYN-180924/2753

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
			Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind (), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**	support/product-security-updates/cve-2024-27364/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27366**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27366/	H-SAM-EXYN-180924/2754
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos	https://semiconductor.samsung.com/support/quality-	H-SAM-EXYN-180924/2755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read. **CVE ID: CVE-2024-27367**	support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27367/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_received_frame_ind(), there is no input validation check on a length coming from	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-180924/2756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27368**		
Product: exynos_1280					
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-180924/2757
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_rx_range_done_ind(), there is no input validation check on rtt_id coming from userspace, which	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27387/	H-SAM-EXYN-180924/2758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can lead to a heap overwrite. **CVE ID: CVE-2024-27387**		
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind (), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27364/	H-SAM-EXYN-180924/2759
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-	H-SAM-EXYN-180924/2760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27366**	updates/cve-2024-27366/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read. **CVE ID: CVE-2024-27367**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27367/	H-SAM-EXYN-180924/2761
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable	https://semiconductor.samsung.com/support/quality-support/produc	H-SAM-EXYN-180924/2762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_received_frame_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27368**	t-security-updates/	
Product: exynos_1330					
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-180924/2763

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
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_rx_range_done_ind(), there is no input validation check on rtt_id coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27387**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27387/	H-SAM-EXYN-180924/2764
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27364/	H-SAM-EXYN-180924/2765

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
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27366**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27366/	H-SAM-EXYN-180924/2766
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27367/	H-SAM-EXYN-180924/2767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read. **CVE ID: CVE-2024-27367**		
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_received_frame_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27368**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-180924/2768
Product: exynos_1380					
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos	https://semiconductor.samsung.com/support/quality-	H-SAM-EXYN-180924/2769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**	support/product-security-updates/	
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_rx_range_done_ind(), there is no input validation check on rtt_id coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27387**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27387/	H-SAM-EXYN-180924/2770
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung	H-SAM-EXYN-180924/2771

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
			Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind (), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**	.com/support/quality-support/product-security-updates/cve-2024-27364/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27366**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27366/	H-SAM-EXYN-180924/2772

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
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read. **CVE ID: CVE-2024-27367**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27367/	H-SAM-EXYN-180924/2773
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_received_fra	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-180924/2774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			me_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27368**		
Product: exynos_1480					
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-180924/2775
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_rx_range_done_ind(), there is no	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-	H-SAM-EXYN-180924/2776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input validation check on rtt_id coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27387**	support/product-security-updates/cve-2024-27387/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind (), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27364/	H-SAM-EXYN-180924/2777
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-	H-SAM-EXYN-180924/2778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27366**	support/product-security-updates/cve-2024-27366/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read. **CVE ID: CVE-2024-27367**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27367/	H-SAM-EXYN-180924/2779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_received_frame_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27368**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-180924/2780
Product: exynos_850					
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-180924/2781

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
			from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**		
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_rx_range_done_ind(), there is no input validation check on rtt_id coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27387**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27387/	H-SAM-EXYN-180924/2782
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind(), there is no input validation check on a length coming from userspace,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27364/	H-SAM-EXYN-180924/2783

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
			which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**		
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27366**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27366/	H-SAM-EXYN-180924/2784
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/produc	H-SAM-EXYN-180924/2785

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
			Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read. **CVE ID: CVE-2024-27367**	t-security-updates/cve-2024-27367/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_received_frame_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27368**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-180924/2786
Product: exynos_980					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-180924/2787
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_rx_range_done_ind(), there is no input validation check on rtt_id coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27387**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27387/	H-SAM-EXYN-180924/2788
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor,	https://semiconductor.samsung.com/support/q	H-SAM-EXYN-180924/2789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind (), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**	uality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27364/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27366/	H-SAM-EXYN-180924/2790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential heap over-read. **CVE ID: CVE-2024-27366**		
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read. **CVE ID: CVE-2024-27367**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27367/	H-SAM-EXYN-180924/2791
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-180924/2792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos W920, Exynos W930. In the function slsi_rx_received_frame_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27368**		
Product: exynos_w920					
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-180924/2793
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and	https://semiconductor.samsung.com/support/quality-support/product-security-updates/,	H-SAM-EXYN-180924/2794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos 1330. In the function slsi_rx_range_done_ind(), there is no input validation check on rtt_id coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27387**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27387/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27364/	H-SAM-EXYN-180924/2795
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos	https://semiconductor.samsung.com/support/quality-support/product-security-updates/,	H-SAM-EXYN-180924/2796

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
			850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27366**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27366/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27367/	H-SAM-EXYN-180924/2797

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
			CVE ID: CVE-2024-27367		
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_received_frame_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27368**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-180924/2798
Product: exynos_w930					
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-180924/2799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input validation check on default_ies coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**		
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_rx_range_done_ind(), there is no input validation check on rtt_id coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27387**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27387/	H-SAM-EXYN-180924/2800
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind(), there is no input	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27364/	H-SAM-EXYN-180924/2801

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
			validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**		
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27366**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27366/	H-SAM-EXYN-180924/2802
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung	H-SAM-EXYN-180924/2803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read. **CVE ID: CVE-2024-27367**	.com/support/quality-support/product-security-updates/cve-2024-27367/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_received_frame_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-180924/2804

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
			CVE ID: CVE-2024-27368		
Vendor: totolink					
Product: t10					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-2024	8.8	A vulnerability, which was classified as critical, was found in TOTOLINK AC1200 T8 and AC1200 T10 4.1.5cu.861_B20230220/4.1.8cu.5207. This affects the function setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument desc leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8573**	N/A	H-TOT-T10-180924/2805
Buffer Copy without Checking Size of Input	08-Sep-2024	8.8	A vulnerability was found in TOTOLINK AC1200 T8 and AC1200 T10 4.1.5cu.861_B20230220/4.1.8cu.5207	N/A	H-TOT-T10-180924/2806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			. It has been classified as critical. Affected is the function setIpPortFilterRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument desc leads to buffer overflow. 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-2024-8576**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-2024	8.8	A vulnerability was found in TOTOLINK AC1200 T8 and AC1200 T10 4.1.5cu.861_B20230220/4.1.8cu.5207. It has been declared as critical. Affected by this vulnerability is the function setStaticDhcpRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument desc leads to buffer overflow. The	N/A	H-TOT-T10-180924/2807

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
			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-2024-8577**		
Product: t8					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-2024	9.8	A vulnerability classified as critical has been found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220. This affects the function setWiFiRepeaterCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument password leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did	N/A	H-TOT-T8-180924/2808

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
			not respond in any way. **CVE ID: CVE-2024-8579**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-2024	8.8	A vulnerability, which was classified as critical, was found in TOTOLINK AC1200 T8 and AC1200 T10 4.1.5cu.861_B20230220/4.1.8cu.5207. This affects the function setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument desc leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8573**	N/A	H-TOT-T8-180924/2809
Improper Neutralization of Special Elements used in an OS Command	08-Sep-2024	8.8	A vulnerability has been found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220 and classified as critical. This vulnerability	N/A	H-TOT-T8-180924/2810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			affects the function setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument slaveIpList leads to os command injection. The attack can 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-2024-8574**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-2024	8.8	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220 and classified as critical. This issue affects the function setWiFiScheduleCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument desc leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may	N/A	H-TOT-T8-180924/2811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8575**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-2024	8.8	A vulnerability was found in TOTOLINK AC1200 T8 and AC1200 T10 4.1.5cu.861_B20230220/4.1.8cu.5207. It has been classified as critical. Affected is the function setIpPortFilterRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument desc leads to buffer overflow. 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-2024-8576**	N/A	H-TOT-T8-180924/2812
Buffer Copy without	08-Sep-2024	8.8	A vulnerability was found in TOTOLINK AC1200 T8 and	N/A	H-TOT-T8-180924/2813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			AC1200 T10 4.1.5cu.861_B20230220/4.1.8cu.5207. It has been declared as critical. Affected by this vulnerability is the function setStaticDhcpRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument desc leads to buffer overflow. 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-2024-8577**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-2024	8.8	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220. It has been rated as critical. Affected by this issue is the function setWiFiMeshName of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument device_name leads	N/A	H-TOT-T8-180924/2814

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
			to buffer overflow. 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-2024-8578**		
Use of Hard-coded Password	08-Sep-2024	8.1	A vulnerability classified as critical was found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220. This vulnerability affects unknown code of the file /etc/shadow.sample. The manipulation leads to use of hard-coded password. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early	N/A	H-TOT-T8-180924/2815

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
			about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8580**		
Vendor: wayos					
Product: fbm-291w					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Sep-2024	6.8	WAYOS FBM-291W v19.09.11 is vulnerable to Command Execution via msp_info_htm. **CVE ID: CVE-2024-44383**	N/A	H-WAY-FBM--180924/2816
Vendor: yubico					
Product: security_key_c_nfc_by_yubico					
Affected Version(s): -					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular	https://www.yubico.com/support/security-advisories/ysa-2024-03/	H-YUB-SECU-180924/2817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**		
Product: security_key_nfc_by_yubico					
Affected Version(s): -					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic	https://www.yubico.com/support/security-advisories/ysa-2024-03/	H-YUB-SECU-180924/2818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			library may also be affected. **CVE ID: CVE-2024-45678**		
Product: yubihsm_2					
Affected Version(s): 2.3.2					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**	https://www.yubico.com/support/security-advisories/ysa-2024-03/	H-YUB-YUBI-180924/2819
Product: yubihsm_2_fips					
Affected Version(s): 2.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**	https://www.yubico.com/support/security-advisories/ysa-2024-03/	H-YUB-YUBI-180924/2820
Product: yubikey_5c					
Affected Version(s): -					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires	https://www.yubico.com/support/security-advisories/ysa-2024-03/	H-YUB-YUBI-180924/2821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**		
Product: yubikey_5ci					
Affected Version(s): -					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the	https://www.yubico.com/support/security-advisories/ysa-2024-03/	H-YUB-YUBI-180924/2822

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
			Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**		
Product: yubikey_5ci_fips					
Affected Version(s): -					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected.	https://www.yubico.com/support/security-advisories/ysa-2024-03/	H-YUB-YUBI-180924/2823

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
			CVE ID: CVE-2024-45678		
Product: yubikey_5c_fips					
Affected Version(s): -					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**	https://www.yubico.com/support/security-advisories/ysa-2024-03/	H-YUB-YUBI-180924/2824
Product: yubikey_5c_nano					
Affected Version(s): -					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with	https://www.yubico.com/support/security-	H-YUB-YUBI-180924/2825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**	advisories/ysa-2024-03/	
Product: yubikey_5c_nano_fips					
Affected Version(s): -					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic	https://www.yubico.com/support/security-advisories/ysa-2024-03/	H-YUB-YUBI-180924/2826

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
			side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**		
Product: yubikey_5c_nfc					
Affected Version(s): -					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an	https://www.yubico.com/support/security-advisories/ysa-2024-03/	H-YUB-YUBI-180924/2827

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
			Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**		
Product: yubikey_5c_nfc_fips					
Affected Version(s): -					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**	https://www.yubico.com/support/security-advisories/ysa-2024-03/	H-YUB-YUBI-180924/2828
Product: yubikey_5_nano					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**	https://www.yubico.com/support/security-advisories/ysa-2024-03/	H-YUB-YUBI-180924/2829
Product: yubikey_5_nano_fips					
Affected Version(s): -					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires	https://www.yubico.com/support/security-advisories/ysa-2024-03/	H-YUB-YUBI-180924/2830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**		
Product: yubikey_5_nfc					
Affected Version(s): -					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the	https://www.yubico.com/support/security-advisories/ysa-2024-03/	H-YUB-YUBI-180924/2831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**		
Product: yubikey_5_nfc_fips					
Affected Version(s): -					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected.	https://www.yubico.com/support/security-advisories/ysa-2024-03/	H-YUB-YUBI-180924/2832

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
			CVE ID: CVE-2024-45678		
Product: yubikey_bio					
Affected Version(s): -					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**	https://www.yubico.com/support/security-advisories/ysa-2024-03/	H-YUB-YUBI-180924/2833
Product: yubikey_c_bio					
Affected Version(s): -					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with	https://www.yubico.com/support/security-	H-YUB-YUBI-180924/2834

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
			firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**	advisories/ysa-2024-03/	
Vendor: Zyxel					
Product: atp100					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	8.1	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP1-180924/2835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username exceeding 28 characters exists. **CVE ID: CVE-2024-42057**		
NULL Pointer Dereference	03-Sep-2024	7.5	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP1-180924/2836

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
			from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through V5.38, USG FLEX series firmware versions from V5.00 through V5.38, USG FLEX 50(W) series firmware versions from V5.00 through V5.38, and USG20(W)-VPN series firmware versions from V5.00 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP1-180924/2837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uploading a crafted compressed language file via FTP. **CVE ID: CVE-2024-42059**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device. **CVE ID: CVE-2024-42060**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP1-180924/2838

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 Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.60 through V5.38 and USG FLEX series firmware versions from V4.60 through V5.38 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device by executing a crafted CLI command. **CVE ID: CVE-2024-7203**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP1-180924/2839
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP1-180924/2840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. The attacker could obtain browser-based information if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP1-180924/2841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-6343**		
Product: atp100w					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	8.1	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP1-180924/2842

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
			authentication mode and a valid user with a long username exceeding 28 characters exists. **CVE ID: CVE-2024-42057**		
NULL Pointer Dereference	03-Sep-2024	7.5	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP1-180924/2843
Improper Neutralization of Special Elements used in an OS	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-	H-ZYX-ATP1-180924/2844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			V5.38, USG FLEX series firmware versions from V5.00 through V5.38, USG FLEX 50(W) series firmware versions from V5.00 through V5.38, and USG20(W)-VPN series firmware versions from V5.00 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted compressed language file via FTP. **CVE ID: CVE-2024-42059**	multiple-vulnerabilities-in-firewalls-09-03-2024	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP1-180924/2845

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
			USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device. **CVE ID: CVE-2024-42060**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.60 through V5.38 and USG FLEX series firmware versions from V4.60 through V5.38 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device by executing a crafted CLI command.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP1-180924/2846

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
			CVE ID: CVE-2024-7203		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. The attacker could obtain browser-based information if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP1-180924/2847
Buffer Copy without Checking Size of	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions	https://www.zyxel.com/global/en/support/security-advisories/zyxe	H-ZYX-ATP1-180924/2848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-6343**	l-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	
Product: atp200					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	8.1	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP2-180924/2849

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
			V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username exceeding 28 characters exists. **CVE ID: CVE-2024-42057**		
NULL Pointer Dereference	03-Sep-2024	7.5	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP2-180924/2850

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
			USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through V5.38, USG FLEX series firmware versions from V5.00 through V5.38, USG FLEX 50(W) series firmware versions from V5.00 through V5.38, and USG20(W)-VPN series firmware versions from V5.00 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted compressed	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP2-180924/2851

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
			language file via FTP. **CVE ID: CVE-2024-42059**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device. **CVE ID: CVE-2024-42060**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP2-180924/2852
Improper Neutralization of Special	03-Sep-2024	7.2	A post-authentication command injection vulnerability in	https://www.zyxel.com/global/en/support/security-	H-ZYX-ATP2-180924/2853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			Zyxel ATP series firmware versions from V4.60 through V5.38 and USG FLEX series firmware versions from V4.60 through V5.38 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device by executing a crafted CLI command. **CVE ID: CVE-2024-7203**	advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP2-180924/2854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. The attacker could obtain browser-based information if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP2-180924/2855

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
			CVE ID: CVE-2024-6343		
Product: atp500					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	8.1	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP5-180924/2856

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
			exceeding 28 characters exists. **CVE ID: CVE-2024-42057**		
NULL Pointer Dereference	03-Sep-2024	7.5	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP5-180924/2857
Improper Neutralization of Special Elements used in an OS Command ('OS	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through V5.38, USG FLEX series firmware versions from V5.00 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-	H-ZYX-ATP5-180924/2858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			V5.38, USG FLEX 50(W) series firmware versions from V5.00 through V5.38, and USG20(W)-VPN series firmware versions from V5.00 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted compressed language file via FTP. **CVE ID: CVE-2024-42059**	in-firewalls-09-03-2024	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP5-180924/2859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device. **CVE ID: CVE-2024-42060**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.60 through V5.38 and USG FLEX series firmware versions from V4.60 through V5.38 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device by executing a crafted CLI command. **CVE ID: CVE-2024-7203**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP5-180924/2860
Improper Neutralization of Input	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the	https://www.zyxel.com/global/en/support/sec	H-ZYX-ATP5-180924/2861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. The attacker could obtain browser-based information if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**	urity-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-	H-ZYX-ATP5-180924/2862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-6343**	in-firewalls-09-03-2024	
Product: atp700					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	8.1	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP7-180924/2863

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
			V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username exceeding 28 characters exists. **CVE ID: CVE-2024-42057**		
NULL Pointer Dereference	03-Sep-2024	7.5	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP7-180924/2864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through V5.38, USG FLEX series firmware versions from V5.00 through V5.38, USG FLEX 50(W) series firmware versions from V5.00 through V5.38, and USG20(W)-VPN series firmware versions from V5.00 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted compressed language file via FTP. **CVE ID: CVE-2024-42059**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP7-180924/2865

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 Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device. **CVE ID: CVE-2024-42060**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP7-180924/2866
Improper Neutralization of Special Elements used in an OS Command	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.60 through V5.38 and USG	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-	H-ZYX-ATP7-180924/2867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			FLEX series firmware versions from V4.60 through V5.38 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device by executing a crafted CLI command. **CVE ID: CVE-2024-7203**	vulnerabilities-in-firewalls-09-03-2024	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP7-180924/2868

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 XSS payload. The attacker could obtain browser-based information if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-6343**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP7-180924/2869
Product: atp800					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	8.1	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username exceeding 28 characters exists.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP8-180924/2870

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
			CVE ID: CVE-2024-42057		
NULL Pointer Dereference	03-Sep-2024	7.5	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP8-180924/2871
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through V5.38, USG FLEX series firmware versions from V5.00 through V5.38, USG FLEX 50(W) series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP8-180924/2872

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
			firmware versions from V5.00 through V5.38, and USG20(W)-VPN series firmware versions from V5.00 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted compressed language file via FTP. **CVE ID: CVE-2024-42059**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP8-180924/2873

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
			attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device. **CVE ID: CVE-2024-42060**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.60 through V5.38 and USG FLEX series firmware versions from V4.60 through V5.38 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device by executing a crafted CLI command. **CVE ID: CVE-2024-7203**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP8-180924/2874
Improper Neutralization of Input During Web Page	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi	https://www.zyxel.com/global/en/support/security-advisories/zyxe	H-ZYX-ATP8-180924/2875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. The attacker could obtain browser-based information if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**	l-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-ATP8-180924/2876

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
			firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-6343**		
Product: ax7501-b0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-AX75-180924/2877
Product: ax7501-b1					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-AX75-180924/2878
Product: dx3300-t0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-DX33-180924/2879
Product: dx3300-t1					
Affected Version(s): -					
Buffer Copy	03-Sep-2024	7.5	A buffer overflow vulnerability in the	https://www.zyxel.com/global/	H-ZYX-DX33-180924/2880

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
without Checking Size of Input ('Classic Buffer Overflow')			library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: dx3301-t0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-DX33-180924/2881
Product: dx4510-b0					
Affected Version(s): -					
Buffer Copy without Checking	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel	https://www.zyxel.com/global/en/support/security-	H-ZYX-DX45-180924/2882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: dx5401-b0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-DX54-180924/2883
Product: dx5401-b1					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-	H-ZYX-DX54-180924/2884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: emg3525-t50b					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-EMG3-180924/2885
Product: emg5523-t50b					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-	H-ZYX-EMG5-180924/2886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: emg5723-t50k					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-EMG5-180924/2887
Product: ex3300-t0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-	H-ZYX-EX33-180924/2888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: ex3300-t1					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-EX33-180924/2889
Product: ex3301-t0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-	H-ZYX-EX33-180924/2890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: ex3500-t0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-EX35-180924/2891
Product: ex3501-t0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-	H-ZYX-EX35-180924/2892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	extender-and-security-router-devices-09-03-2024	
Product: ex3510-b0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-EX35-180924/2893
Product: ex5401-b0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-	H-ZYX-EX54-180924/2894

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
			CVE ID: CVE-2024-5412	devices-09-03-2024	
Product: ex5401-b1					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-EX54-180924/2895
Product: ex5510-b0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-EX55-180924/2896

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
Product: ex5512-t0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-EX55-180924/2897
Product: ex5601-t0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-EX56-180924/2898
Product: ex5601-t1					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-EX56-180924/2899
Product: ex7501-b0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-EX75-180924/2900
Product: ex7710-b0					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-EX77-180924/2901
Product: nebula_fwa505					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-NEBU-180924/2902
Product: nebula_fwa510					
Affected Version(s): -					
Buffer Copy	03-Sep-2024	7.5	A buffer overflow vulnerability in the	https://www.zyxel.com/global/	H-ZYX-NEBU-180924/2903

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
without Checking Size of Input ('Classic Buffer Overflow')			library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: nebula_fwa710					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-NEBU-180924/2904
Product: nebula_lte3301-plus					
Affected Version(s): -					
Buffer Copy without Checking	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel	https://www.zyxel.com/global/en/support/security-	H-ZYX-NEBU-180924/2905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: nr5103					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-NR51-180924/2906
Product: nr5103ev2					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-	H-ZYX-NR51-180924/2907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: nr5307					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-NR53-180924/2908
Product: nr7103					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-	H-ZYX-NR71-180924/2909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: nr7302					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-NR73-180924/2910
Product: nr7303					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-	H-ZYX-NR73-180924/2911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: nr7501					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-NR75-180924/2912
Product: nwa110ax					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4)	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-	H-ZYX-NWA1-180924/2913

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
			and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP .2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	devices-09-03-2024	
Product: nwa1123-ac_pro					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-NWA1-180924/2914

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
			earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP .2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: nwa1123acv3					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1)	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-NWA1-180924/2915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, and USG LITE 60AX firmware version V2.00(ACIP .2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: nwa130be					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP .2) could allow an	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-NWA1-180924/2916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: nwa210ax					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-NWA2-180924/2917

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
			cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: nwa220ax-6e					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-NWA2-180924/2918

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
Product: nwa50ax					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-NWA5-180924/2919
Product: nwa50ax_pro					
Affected Version(s): -					
Improper Neutralization of	03-Sep-2024	9.8	The improper neutralization of special elements in	https://www.zyxel.com/global/en/support/sec	H-ZYX-NWA5-180924/2920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	urity-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	
Product: nwa55axe					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-	H-ZYX-NWA5-180924/2921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	
Product: nwa90ax					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4)	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-	H-ZYX-NWA9-180924/2922

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
			and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	devices-09-03-2024	
Product: nwa90ax_pro					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-NWA9-180924/2923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP .2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: pm3100-t0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-PM31-180924/2924
Product: pm5100-t0					
Affected Version(s): -					
Buffer Copy without	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc"	https://www.zyxel.com/global/en/support/sec	H-ZYX-PM51-180924/2925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	urity-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: pm7300-t0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-PM73-180924/2926
Product: px3321-t1					
Affected Version(s): -					
Buffer Copy without Checking Size of	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K	https://www.zyxel.com/global/en/support/security-advisories/zyxe	H-ZYX-PX33-180924/2927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	l-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: scr50axe					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-SCR5-180924/2928
Product: usg_20w-vpn					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	03-Sep-2024	8.1	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-	H-ZYX-USG_-180924/2929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username exceeding 28 characters exists. **CVE ID: CVE-2024-42057**	multiple-vulnerabilities-in-firewalls-09-03-2024	
NULL Pointer Dereference	03-Sep-2024	7.5	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-	H-ZYX-USG_-180924/2930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**	multiple-vulnerabilities-in-firewalls-09-03-2024	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through V5.38, USG FLEX series firmware versions from V5.00 through V5.38, USG FLEX 50(W) series firmware versions from V5.00 through V5.38, and USG20(W)-VPN series firmware versions from V5.00 through V5.38 could allow an authenticated	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2931

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
			attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted compressed language file via FTP. **CVE ID: CVE-2024-42059**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2932

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 vulnerable device. **CVE ID: CVE-2024-42060**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. The attacker could obtain browser-based information if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2933
Buffer Copy without	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of	https://www.zyxel.com/global/en/support/sec	H-ZYX-USG_-180924/2934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-6343**	urity-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	
Product: usg_flex_100					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	8.1	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2935

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
			firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username exceeding 28 characters exists. **CVE ID: CVE-2024-42057**		
NULL Pointer Dereference	03-Sep-2024	7.5	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2936

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
			from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through V5.38, USG FLEX series firmware versions from V5.00 through V5.38, USG FLEX 50(W) series firmware versions from V5.00 through V5.38, and USG20(W)-VPN series firmware versions from V5.00 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uploading a crafted compressed language file via FTP. **CVE ID: CVE-2024-42059**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device. **CVE ID: CVE-2024-42060**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2938

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 Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.60 through V5.38 and USG FLEX series firmware versions from V4.60 through V5.38 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device by executing a crafted CLI command. **CVE ID: CVE-2024-7203**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2939
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2940

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
			USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. The attacker could obtain browser-based information if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-6343**		
Product: usg_flex_100ax					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	8.1	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2942

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
			authentication mode and a valid user with a long username exceeding 28 characters exists. **CVE ID: CVE-2024-42057**		
NULL Pointer Dereference	03-Sep-2024	7.5	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2943
Improper Neutralization of Special Elements used in an OS	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-	H-ZYX-USG_-180924/2944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			V5.38, USG FLEX series firmware versions from V5.00 through V5.38, USG FLEX 50(W) series firmware versions from V5.00 through V5.38, and USG20(W)-VPN series firmware versions from V5.00 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted compressed language file via FTP. **CVE ID: CVE-2024-42059**	multiple-vulnerabilities-in-firewalls-09-03-2024	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2945

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
			USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device. **CVE ID: CVE-2024-42060**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.60 through V5.38 and USG FLEX series firmware versions from V4.60 through V5.38 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device by executing a crafted CLI command.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2946

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
			CVE ID: CVE-2024-7203		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. The attacker could obtain browser-based information if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2947
Buffer Copy without Checking Size of	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions	https://www.zyxel.com/global/en/support/security-advisories/zyxe	H-ZYX-USG_-180924/2948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-6343**	l-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	
Product: usg_flex_100w					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	8.1	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2949

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
			V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username exceeding 28 characters exists. **CVE ID: CVE-2024-42057**		
NULL Pointer Dereference	03-Sep-2024	7.5	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2950

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
			USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through V5.38, USG FLEX series firmware versions from V5.00 through V5.38, USG FLEX 50(W) series firmware versions from V5.00 through V5.38, and USG20(W)-VPN series firmware versions from V5.00 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted compressed	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2951

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
			language file via FTP. **CVE ID: CVE-2024-42059**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device. **CVE ID: CVE-2024-42060**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2952
Improper Neutralization of Special	03-Sep-2024	7.2	A post-authentication command injection vulnerability in	https://www.zyxel.com/global/en/support/security-	H-ZYX-USG_-180924/2953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			Zyxel ATP series firmware versions from V4.60 through V5.38 and USG FLEX series firmware versions from V4.60 through V5.38 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device by executing a crafted CLI command. **CVE ID: CVE-2024-7203**	advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. The attacker could obtain browser-based information if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2955

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
			CVE ID: CVE-2024-6343		
Product: usg_flex_200					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	8.1	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2956

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
			exceeding 28 characters exists. **CVE ID: CVE-2024-42057**		
NULL Pointer Dereference	03-Sep-2024	7.5	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2957
Improper Neutralization of Special Elements used in an OS Command ('OS	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through V5.38, USG FLEX series firmware versions from V5.00 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-	H-ZYX-USG_-180924/2958

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
Command Injection')			V5.38, USG FLEX 50(W) series firmware versions from V5.00 through V5.38, and USG20(W)-VPN series firmware versions from V5.00 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted compressed language file via FTP. **CVE ID: CVE-2024-42059**	in-firewalls-09-03-2024	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device. **CVE ID: CVE-2024-42060**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.60 through V5.38 and USG FLEX series firmware versions from V4.60 through V5.38 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device by executing a crafted CLI command. **CVE ID: CVE-2024-7203**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2960
Improper Neutralization of Input	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the	https://www.zyxel.com/global/en/support/sec	H-ZYX-USG_-180924/2961

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
During Web Page Generation ('Cross-site Scripting')			CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. The attacker could obtain browser-based information if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**	urity-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-	H-ZYX-USG_-180924/2962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-6343**	in-firewalls-09-03-2024	
Product: usg_flex_50					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	8.1	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2963

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
			V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username exceeding 28 characters exists. **CVE ID: CVE-2024-42057**		
NULL Pointer Dereference	03-Sep-2024	7.5	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through V5.38, USG FLEX series firmware versions from V5.00 through V5.38, USG FLEX 50(W) series firmware versions from V5.00 through V5.38, and USG20(W)-VPN series firmware versions from V5.00 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted compressed language file via FTP. **CVE ID: CVE-2024-42059**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2965

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 Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device. **CVE ID: CVE-2024-42060**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2966
Improper Neutralization of Special Elements used in an OS Command	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.60 through V5.38 and USG	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-	H-ZYX-USG_-180924/2967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			FLEX series firmware versions from V4.60 through V5.38 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device by executing a crafted CLI command. **CVE ID: CVE-2024-7203**	vulnerabilities-in-firewalls-09-03-2024	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2968

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 XSS payload. The attacker could obtain browser-based information if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-6343**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2969
Product: usg_flex_500					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	8.1	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username exceeding 28 characters exists.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2970

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
			CVE ID: CVE-2024-42057		
NULL Pointer Dereference	03-Sep-2024	7.5	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2971
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through V5.38, USG FLEX series firmware versions from V5.00 through V5.38, USG FLEX 50(W) series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2972

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
			firmware versions from V5.00 through V5.38, and USG20(W)-VPN series firmware versions from V5.00 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted compressed language file via FTP. **CVE ID: CVE-2024-42059**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2973

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
			attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device. **CVE ID: CVE-2024-42060**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.60 through V5.38 and USG FLEX series firmware versions from V4.60 through V5.38 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device by executing a crafted CLI command. **CVE ID: CVE-2024-7203**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2974
Improper Neutralization of Input During Web Page	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi	https://www.zyxel.com/global/en/support/security-advisories/zyxe	H-ZYX-USG_-180924/2975

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
Generation ('Cross-site Scripting')			" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. The attacker could obtain browser-based information if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**	l-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2976

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
			firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-6343**		
Product: usg_flex_50w					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	8.1	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2977

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
			attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username exceeding 28 characters exists. **CVE ID: CVE-2024-42057**		
NULL Pointer Dereference	03-Sep-2024	7.5	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2978

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
			DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through V5.38, USG FLEX series firmware versions from V5.00 through V5.38, USG FLEX 50(W) series firmware versions from V5.00 through V5.38, and USG20(W)-VPN series firmware versions from V5.00 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted compressed language file via FTP. **CVE ID: CVE-2024-42059**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2979
Improper Neutralization of	03-Sep-2024	7.2	A post-authentication command injection	https://www.zyxel.com/global/en/support/sec	H-ZYX-USG_-180924/2980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device. **CVE ID: CVE-2024-42060**	urity-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.60 through V5.38 and USG FLEX series firmware versions from V4.60 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2981

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
			V5.38 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device by executing a crafted CLI command. **CVE ID: CVE-2024-7203**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. The attacker could obtain browser-	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2982

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
			based information if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-6343**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2983
Product: usg_flex_700					
Affected Version(s): -					
Improper Neutralizat	03-Sep-2024	8.1	A command injection	https://www.zyxel.com/global/	H-ZYX-USG_-180924/2984

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
ion of Special Elements used in an OS Command ('OS Command Injection')			vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username exceeding 28 characters exists. **CVE ID: CVE-2024-42057**	en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	
NULL Pointer	03-Sep-2024	7.5	A null pointer dereference	https://www.zyxel.com/global/	H-ZYX-USG_-180924/2985

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			vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**	en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through V5.38, USG FLEX series firmware versions from V5.00 through V5.38, USG FLEX 50(W) series firmware versions from V5.00 through V5.38, and USG20(W)-VPN	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2986

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
			series firmware versions from V5.00 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted compressed language file via FTP. **CVE ID: CVE-2024-42059**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device. **CVE ID: CVE-2024-42060**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.60 through V5.38 and USG FLEX series firmware versions from V4.60 through V5.38 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device by executing a crafted CLI command. **CVE ID: CVE-2024-7203**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2988
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-	H-ZYX-USG_-180924/2989

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
			V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. The attacker could obtain browser-based information if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**	in-firewalls-09-03-2024	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	H-ZYX-USG_-180924/2990

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
			series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-6343**		
Product: usg_lite_60ax					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-USG_-180924/2991

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
			version V2.00(ACIP .2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: vmg3625-t50b					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-VMG3-180924/2992
Product: vmg3927-t50k					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-	H-ZYX-VMG3-180924/2993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: vmg4005-b50a					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-VMG4-180924/2994
Product: vmg4005-b60a					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-	H-ZYX-VMG4-180924/2995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: vmg8623-t50b					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-VMG8-180924/2996
Product: vmg8825-t50k					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-	H-ZYX-VMG8-180924/2997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	extender-and-security-router-devices-09-03-2024	
Product: wac500					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-WAC5-180924/2998

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
Product: wac500h					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-WAC5-180924/2999
Product: wac6103d-i					
Affected Version(s): -					
Improper Neutralization of	03-Sep-2024	9.8	The improper neutralization of special elements in	https://www.zyxel.com/global/en/support/sec	H-ZYX-WAC6-180924/3000

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
Special Elements used in an OS Command ('OS Command Injection')			the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	urity-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	
Product: wac6502d-s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-	H-ZYX-WAC6-180924/3001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	
Product: wac6503d-s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4)	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-	H-ZYX-WAC6-180924/3002

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
			and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	devices-09-03-2024	
Product: wac6552d-s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-WAC6-180924/3003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: wac6553d-e					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-WAC6-180924/3004

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
			firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: wax300h					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-WAX3-180924/3005

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
			OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: wax510d					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-WAX5-180924/3006

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
			CVE ID: CVE-2024-7261		
Product: wax610d					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-WAX6-180924/3007
Product: wax620d-6e					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-WAX6-180924/3008
Product: wax630s					
Affected Version(s): -					
Improper Neutralization of Special Elements	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI	https://www.zyxel.com/global/en/support/security-advisories/zyxe	H-ZYX-WAX6-180924/3009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	l-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	
Product: wax640s-6e					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-	H-ZYX-WAX6-180924/3010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP .2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	aps-and-security-router-devices-09-03-2024	
Product: wax650s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-WAX6-180924/3011

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
			firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: wax655e					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1)	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-WAX6-180924/3012

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
			and earlier, and USG LITE 60AX firmware version V2.00(ACIP .2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: wbe530					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-WBE5-180924/3013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: wbe660s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP .2) could allow an unauthenticated attacker to execute OS commands by sending a crafted	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	H-ZYX-WBE6-180924/3014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: wx3100-t0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-WX31-180924/3015
Product: wx3401-b0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-	H-ZYX-WX34-180924/3016

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
			CVE ID: CVE-2024-5412	devices-09-03-2024	
Product: wx5600-t0					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	H-ZYX-WX56-180924/3017
Operating System					
Vendor: Apple					
Product: macos					
Affected Version(s): -					
Out-of-bounds Write	13-Sep-2024	7.8	Media Encoder versions 24.5, 23.6.8 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	O-APP-MACO-190924/3018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID: CVE-2024-39377**		
Out-of-bounds Read	13-Sep-2024	7.8	Media Encoder versions 24.5, 23.6.8 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2024-41871**	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	O-APP-MACO-190924/3019
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Sep-2024	7.8	After Effects versions 23.6.6, 24.5 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	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	O-APP-MACO-190924/3020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39380**		
Out-of-bounds Write	13-Sep-2024	7.8	After Effects versions 23.6.6, 24.5 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-2024-39381**	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	O-APP-MACO-190924/3021
Out-of-bounds Write	13-Sep-2024	7.8	Premiere Pro versions 24.5, 23.6.8 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-2024-39384**	https://helpx.adobe.com/security/products/premiere_pro/apsb24-58.html	O-APP-MACO-190924/3022

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 Underflow (Wrap or Wraparound)	13-Sep-2024	7.8	Illustrator versions 28.6, 27.9.5 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-2024-41857**	https://helpx.adobe.com/security/products/illustrator/apsb24-66.html	O-APP-MACO-190924/3023
Out-of-bounds Write	13-Sep-2024	7.8	After Effects versions 23.6.6, 24.5 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-2024-41859**	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	O-APP-MACO-190924/3024
Use After Free	13-Sep-2024	7.8	Illustrator versions 28.6, 27.9.5 and earlier are affected by a Use After Free vulnerability that could result in	https://helpx.adobe.com/security/products/illustrator/apsb24-66.html	O-APP-MACO-190924/3025

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
			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-2024-43758**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Sep-2024	7.8	Photoshop Desktop versions 24.7.4, 25.11 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-2024-43756**	https://helpx.adobe.com/security/products/photoshop/apsb24-72.html	O-APP-MACO-190924/3026
Out-of-bounds Write	13-Sep-2024	7.8	Photoshop Desktop versions 24.7.4, 25.11 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	https://helpx.adobe.com/security/products/photoshop/apsb24-72.html	O-APP-MACO-190924/3027

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
			interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-43760**		
Out-of-bounds Write	13-Sep-2024	7.8	Photoshop Desktop versions 24.7.4, 25.11 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-2024-45108**	https://helpx.adobe.com/security/products/photoshop/apsb24-72.html	O-APP-MACO-190924/3028
Out-of-bounds Write	13-Sep-2024	7.8	Photoshop Desktop versions 24.7.4, 25.11 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-2024-45109**	https://helpx.adobe.com/security/products/photoshop/apsb24-72.html	O-APP-MACO-190924/3029

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
Use After Free	05-Sep-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20964, 24.001.30123, 24.002.20991 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-45107**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-APP-MACO-190924/3030
Out-of-bounds Read	13-Sep-2024	5.5	Media Encoder versions 24.5, 23.6.8 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	O-APP-MACO-190924/3031

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
			CVE ID: CVE-2024-41870		
Out-of-bounds Read	13-Sep-2024	5.5	Media Encoder versions 24.5, 23.6.8 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-2024-41872**	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	O-APP-MACO-190924/3032
Out-of-bounds Read	13-Sep-2024	5.5	Media Encoder versions 24.5, 23.6.8 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	O-APP-MACO-190924/3033

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
			CVE ID: CVE-2024-41873		
Out-of-bounds Read	13-Sep-2024	5.5	After Effects versions 23.6.6, 24.5 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-2024-39382**	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	O-APP-MACO-190924/3034
Use After Free	13-Sep-2024	5.5	Premiere Pro versions 24.5, 23.6.8 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/premiere_pro/apsb24-58.html	O-APP-MACO-190924/3035

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
			CVE ID: CVE-2024-39385		
Out-of-bounds Read	13-Sep-2024	5.5	After Effects versions 23.6.6, 24.5 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-2024-41867**	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	O-APP-MACO-190924/3036
NULL Pointer Dereference	13-Sep-2024	5.5	Illustrator versions 28.6, 27.9.5 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a DoS condition. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/illustrator/apsb24-66.html	O-APP-MACO-190924/3037

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
			victim must open a malicious file. **CVE ID: CVE-2024-43759**		
Out-of-bounds Read	13-Sep-2024	5.5	Illustrator versions 28.6, 27.9.5 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-2024-45111**	https://helpx.adobe.com/security/products/illustrator/apsb24-66.html	O-APP-MACO-190924/3038
Vendor: comfast					
Product: cf-xr11_firmware					
Affected Version(s): 2.7.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-Sep-2024	9.8	COMFAST CF-XR11 V2.7.2 has a command injection vulnerability in function sub_424CB4. Attackers can send POST request messages to /usr/bin/webmgnt and inject commands into parameter iface.	N/A	O-COM-CF-X-190924/3039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-44466		
Vendor: crucial					
Product: mx500_firmware					
Affected Version(s): m3cr046					
Out-of-bounds Write	04-Sep-2024	6.7	Micron Crucial MX500 Series Solid State Drives M3CR046 is vulnerable to Buffer Overflow, which can be triggered by sending specially crafted ATA packets from the host to the drive controller. **CVE ID: CVE-2024-42642**	N/A	O-CRU-MX50-190924/3040
Vendor: Dell					
Product: 7920_xl_firmware					
Affected Version(s): * Up to (excluding) 2.22.1					
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Sep-2024	5.5	Dell Precision Rack, 14G Intel BIOS versions prior to 2.22.2, contains an Access of Memory Location After End of Buffer vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	https://www.dell.com/support/kbdoc/en-us/000227015/dsa-2024-328	O-DEL-7920-190924/3041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42425		
Product: precision_7920_firmware					
Affected Version(s): * Up to (excluding) 2.22.1					
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Sep-2024	5.5	Dell Precision Rack, 14G Intel BIOS versions prior to 2.22.2, contains an Access of Memory Location After End of Buffer vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure. **CVE ID: CVE-2024-42425**	https://www.dell.com/support/kbdoc/en-us/000227015/dsa-2024-328	O-DEL-PREC-190924/3042
Product: smartfabric_os10					
Affected Version(s): From (including) 10.5.5.4 Up to (including) 10.5.5.10					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Sep-2024	8.8	Dell SmartFabric OS10 Software, version(s) 10.5.5.4 through 10.5.5.10 and 10.5.6.x , contain(s) an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability,	https://www.dell.com/support/kbdoc/en-us/000228355/dsa-2024-376-security-update-for-dell-networking-os10-vulnerability	O-DEL-SMAR-190924/3043

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
			leading to Command execution. **CVE ID: CVE-2024-38486**		
Use of Hard-coded Credentials	06-Sep-2024	8.1	Dell SmartFabric OS10 Software, version(s) 10.5.5.4 through 10.5.5.10 and 10.5.6.x, contain(s) an Use of Hard-coded Password vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Client-side request forgery and Information disclosure. **CVE ID: CVE-2024-39585**	https://www.dell.com/support/kbdoc/en-us/000228355/dsa-2024-376-security-update-for-dell-networking-os10-vulnerability	O-DEL-SMAR-190924/3044
Affected Version(s): From (including) 10.5.6.0 Up to (excluding) 10.5.6.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Sep-2024	8.8	Dell SmartFabric OS10 Software, version(s) 10.5.5.4 through 10.5.5.10 and 10.5.6.x , contain(s) an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. A low privileged attacker with remote access	https://www.dell.com/support/kbdoc/en-us/000228355/dsa-2024-376-security-update-for-dell-networking-os10-vulnerability	O-DEL-SMAR-190924/3045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could potentially exploit this vulnerability, leading to Command execution. **CVE ID: CVE-2024-38486**		
Use of Hard-coded Credentials	06-Sep-2024	8.1	Dell SmartFabric OS10 Software, version(s) 10.5.5.4 through 10.5.5.10 and 10.5.6.x, contain(s) an Use of Hard-coded Password vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Client-side request forgery and Information disclosure. **CVE ID: CVE-2024-39585**	https://www.dell.com/support/kbdoc/en-us/000228355/dsa-2024-376-security-update-for-dell-networking-os10-vulnerability	O-DEL-SMAR-190924/3046
Vendor: Dlink					
Product: di-8100g_firmware					
Affected Version(s): 17.12.20a1					
Improper Neutralization of Special Elements used in a Command ('Comman	06-Sep-2024	9.8	D-Link DI-8100G 17.12.20A1 is vulnerable to Command Injection via sub47A60C function in the upgrade_filter.asp file	N/A	O-DLI-DI-8-190924/3047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			**CVE ID: CVE-2024-44401**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Sep-2024	9.8	D-Link DI-8100G 17.12.20A1 is vulnerable to Command Injection via msp_info.htm. **CVE ID: CVE-2024-44402**	N/A	O-DLI-DI-8-190924/3048
Product: di-8300_firmware					
Affected Version(s): 16.07.26a1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-Sep-2024	9.8	D-Link DI-8300 v16.07.26A1 is vulnerable to command injection via the upgrade_filter_asp function. **CVE ID: CVE-2024-44410**	N/A	O-DLI-DI-8-190924/3049
Product: di-8400_firmware					
Affected Version(s): 16.07.26a1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Sep-2024	9.8	D-Link DI-8400 16.07.26A1 is vulnerable to Command Injection via upgrade_filter_asp. **CVE ID: CVE-2024-44400**	N/A	O-DLI-DI-8-190924/3050
Product: dir-823g_firmware					
Affected Version(s): 1.0.2b05_20181207					

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
Missing Authorization	06-Sep-2024	7.5	D-Link DIR-823G v1.0.2B05_20181207 is vulnerable to Information Disclosure. The device allows unauthorized configuration file downloads, and the downloaded configuration files contain plaintext user passwords. **CVE ID: CVE-2024-44408**	N/A	O-DLI-DIR--190924/3051
Product: dns-320_firmware					
Affected Version(s): 2.02b01					
N/A	05-Sep-2024	5.9	A vulnerability, which was classified as problematic, has been found in D-Link DNS-320 2.02b01. Affected by this issue is some unknown functionality of the file /cgi-bin/widget_api.cgi of the component Web Management Interface. The manipulation of the argument getHD/getSer/getSys leads to information disclosure. The attack may be launched remotely. The complexity of an attack is rather high. The	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--190924/3052

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
			exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8460**		
N/A	05-Sep-2024	5.3	A vulnerability, which was classified as problematic, was found in D-Link DNS-320 2.02b01. This affects an unknown part of the file /cgi-bin/discovery.cgi of the component Web Management Interface. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This	N/A	O-DLI-DNS--190924/3053

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
			vulnerability only affects products that are no longer supported by the maintainer. Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8461**		
Vendor: Draytek					
Product: vigor3900_firmware					
Affected Version(s): 1.5.1.6					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	DrayTek Vigor3900 v1.5.1.6 was discovered to contain an authenticated command injection vulnerability via the name parameter in the run_command function. **CVE ID: CVE-2024-44844**	N/A	O-DRA-VIGO-190924/3054
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	DrayTek Vigor3900 v1.5.1.6 was discovered to contain an authenticated command injection vulnerability via the value parameter in the filter_string function.	N/A	O-DRA-VIGO-190924/3055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-44845		
Vendor: Freebsd					
Product: freebsd					
Affected Version(s): 13.3					
Improper Validation of Specified Quantity in Input	05-Sep-2024	8.8	The ctl_report_supported_opcodes function did not sufficiently validate a field provided by userspace, allowing an arbitrary write to a limited amount of kernel help memory. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host.	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3056

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
			CVE ID: CVE-2024-42416		
Out-of-bounds Read	05-Sep-2024	8.8	The ctl_request_sense function could expose up to three bytes of the kernel heap to userspace. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host. **CVE ID: CVE-2024-43110**	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3057
Use After Free	05-Sep-2024	8.8	The function ctl_write_buffer incorrectly set a flag which resulted in a kernel Use-After-Free when a	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command finished processing. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host. **CVE ID: CVE-2024-45063**		
Missing Initialization of Resource	05-Sep-2024	8.8	The ctl_write_buffer and ctl_read_buffer functions allocated memory to be returned to userspace, without initializing it. Malicious software running in a guest VM that exposes	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3059

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
			virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host. **CVE ID: CVE-2024-8178**		
Out-of-bounds Write	05-Sep-2024	8.2	An insufficient boundary validation in the USB code could lead to an out-of-bounds write on the heap, with data controlled by the caller. A malicious, privileged software running in a guest VM can exploit the vulnerability to achieve code execution on the host in the bhyve userspace process,	https://security.freebsd.org/advisories/FreeBSD-SA-24:12.bhyve.asc	O-FRE-FREE-190924/3060

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
			which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. **CVE ID: CVE-2024-32668**		
Integer Overflow or Wraparound	05-Sep-2024	7.5	A malicious value of size in a structure of packed libnv can cause an integer overflow, leading to the allocation of a smaller buffer than required for the parsed data. **CVE ID: CVE-2024-45287**	https://security.freebsd.org/advisories/FreeBSD-SA-24:09.libnv.asc	O-FRE-FREE-190924/3061
Use After Free	05-Sep-2024	10	Concurrent removals of certain anonymous shared memory mappings by using the UMTX_SHM_DESTROY sub-request of UMTX_OP_SHM can lead to decreasing the reference count of the object representing the mapping too many times, causing it to be freed too early. A malicious code exercizing the UMTX_SHM_DESTROY sub-request in	https://security.freebsd.org/advisories/FreeBSD-SA-24:14.umtx.asc	O-FRE-FREE-190924/3062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parallel can panic the kernel or enable further Use-After-Free attacks, potentially including code execution or Capsicum sandbox escape. **CVE ID: CVE-2024-43102**		
Affected Version(s): 13.4					
Improper Validation of Specified Quantity in Input	05-Sep-2024	8.8	The ctl_report_supported_opcodes function did not sufficiently validate a field provided by userspace, allowing an arbitrary write to a limited amount of kernel help memory. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host. **CVE ID: CVE-2024-42416**		
Out-of-bounds Read	05-Sep-2024	8.8	The ctl_request_sense function could expose up to three bytes of the kernel heap to userspace. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host.	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3064

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
			CVE ID: CVE-2024-43110		
Use After Free	05-Sep-2024	8.8	The function ctl_write_buffer incorrectly set a flag which resulted in a kernel Use-After-Free when a command finished processing. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host. **CVE ID: CVE-2024-45063**	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3065
Missing Initialization of Resource	05-Sep-2024	8.8	The ctl_write_buffer and ctl_read_buffer functions allocated	https://security.freebsd.org/advisories/FreeBS	O-FRE-FREE-190924/3066

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
			memory to be returned to userspace, without initializing it. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host. **CVE ID: CVE-2024-8178**	D-SA-24:11.ctl.asc	
Out-of-bounds Write	05-Sep-2024	8.2	An insufficient boundary validation in the USB code could lead to an out-of-bounds write on the heap, with data controlled by the caller.	https://security.freebsd.org/advisories/FreeBSD-SA-24:12.bhyve.asc	O-FRE-FREE-190924/3067

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
			A malicious, privileged software running in a guest VM can exploit the vulnerability to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. **CVE ID: CVE-2024-32668**		
Integer Overflow or Wraparound	05-Sep-2024	7.5	A malicious value of size in a structure of packed libnv can cause an integer overflow, leading to the allocation of a smaller buffer than required for the parsed data. **CVE ID: CVE-2024-45287**	https://security.freebsd.org/advisories/FreeBSD-SA-24:09.libnv.asc	O-FRE-FREE-190924/3068
Use After Free	05-Sep-2024	10	Concurrent removals of certain anonymous shared memory mappings by using the UMTX_SHM_DESTROY sub-request of UMTX_OP_SHM can lead to decreasing the reference count of the object representing the	https://security.freebsd.org/advisories/FreeBSD-SA-24:14.umtx.asc	O-FRE-FREE-190924/3069

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
			mapping too many times, causing it to be freed too early. A malicious code exercizing the UMTX_SHM_DESTROY sub-request in parallel can panic the kernel or enable further Use-After-Free attacks, potentially including code execution or Capsicum sandbox escape. **CVE ID: CVE-2024-43102**		
Affected Version(s): 14.0					
Improper Validation of Specified Quantity in Input	05-Sep-2024	8.8	The ctl_report_supported_opcodes function did not sufficiently validate a field provided by userspace, allowing an arbitrary write to a limited amount of kernel help memory. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process,	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3070

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
			which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host. **CVE ID: CVE-2024-42416**		
Out-of-bounds Read	05-Sep-2024	8.8	The ctl_request_sense function could expose up to three bytes of the kernel heap to userspace. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3071

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
			malicious iSCSI initiator could achieve remote code execution on the iSCSI target host. **CVE ID: CVE-2024-43110**		
Use After Free	05-Sep-2024	8.8	The function ctl_write_buffer incorrectly set a flag which resulted in a kernel Use-After-Free when a command finished processing. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host.	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3072

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
			CVE ID: CVE-2024-45063		
Missing Initialization of Resource	05-Sep-2024	8.8	The ctl_write_buffer and ctl_read_buffer functions allocated memory to be returned to userspace, without initializing it. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host. **CVE ID: CVE-2024-8178**	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3073
Out-of-bounds Write	05-Sep-2024	8.2	An insufficient boundary validation in the USB code could	https://security.freebsd.org/advisories/FreeBS	O-FRE-FREE-190924/3074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to an out-of-bounds write on the heap, with data controlled by the caller. A malicious, privileged software running in a guest VM can exploit the vulnerability to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. **CVE ID: CVE-2024-32668**	D-SA-24:12.bhyve.asc	
Integer Overflow or Wraparound	05-Sep-2024	7.5	A malicious value of size in a structure of packed libnv can cause an integer overflow, leading to the allocation of a smaller buffer than required for the parsed data. **CVE ID: CVE-2024-45287**	https://security.freebsd.org/advisories/FreeBSD-SA-24:09.libnv.asc	O-FRE-FREE-190924/3075
Use After Free	05-Sep-2024	10	Concurrent removals of certain anonymous shared memory mappings by using the	https://security.freebsd.org/advisories/FreeBSD-SA-24:14.umtx.asc	O-FRE-FREE-190924/3076

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
			UMTX_SHM_DESTROY sub-request of UMTX_OP_SHM can lead to decreasing the reference count of the object representing the mapping too many times, causing it to be freed too early. A malicious code exercizing the UMTX_SHM_DESTROY sub-request in parallel can panic the kernel or enable further Use-After-Free attacks, potentially including code execution or Capsicum sandbox escape. **CVE ID: CVE-2024-43102**		
Affected Version(s): 14.1					
Improper Validation of Specified Quantity in Input	05-Sep-2024	8.8	The ctl_report_supported_opcodes function did not sufficiently validate a field provided by userspace, allowing an arbitrary write to a limited amount of kernel help memory. Malicious software running in a guest VM that exposes	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3077

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
			virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host. **CVE ID: CVE-2024-42416**		
Out-of-bounds Read	05-Sep-2024	8.8	The ctl_request_sense function could expose up to three bytes of the kernel heap to userspace. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host. **CVE ID: CVE-2024-43110**		
Use After Free	05-Sep-2024	8.8	The function ctl_write_buffer incorrectly set a flag which resulted in a kernel Use-After-Free when a command finished processing. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3079

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
			malicious iSCSI initiator could achieve remote code execution on the iSCSI target host. **CVE ID: CVE-2024-45063**		
Missing Initialization of Resource	05-Sep-2024	8.8	The ctl_write_buffer and ctl_read_buffer functions allocated memory to be returned to userspace, without initializing it. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host.	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3080

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
			CVE ID: CVE-2024-8178		
Out-of-bounds Write	05-Sep-2024	8.2	An insufficient boundary validation in the USB code could lead to an out-of-bounds write on the heap, with data controlled by the caller. A malicious, privileged software running in a guest VM can exploit the vulnerability to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. **CVE ID: CVE-2024-32668**	https://security.freebsd.org/advisories/FreeBSD-SA-24:12.bhyve.asc	O-FRE-FREE-190924/3081
Integer Overflow or Wraparound	05-Sep-2024	7.5	A malicious value of size in a structure of packed libnv can cause an integer overflow, leading to the allocation of a smaller buffer than required for the parsed data.	https://security.freebsd.org/advisories/FreeBSD-SA-24:09.libnv.asc	O-FRE-FREE-190924/3082

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
			CVE ID: CVE-2024-45287		
Use After Free	05-Sep-2024	10	Concurrent removals of certain anonymous shared memory mappings by using the UMTX_SHM_DESTROY sub-request of UMTX_OP_SHM can lead to decreasing the reference count of the object representing the mapping too many times, causing it to be freed too early. A malicious code exercizing the UMTX_SHM_DESTROY sub-request in parallel can panic the kernel or enable further Use-After-Free attacks, potentially including code execution or Capsicum sandbox escape. **CVE ID: CVE-2024-43102**	https://security.freebsd.org/advisories/FreeBSD-SA-24:14.umtx.asc	O-FRE-FREE-190924/3083
Affected Version(s): From (including) 13.0 Up to (excluding) 13.3					
Improper Validation of Specified Quantity in Input	05-Sep-2024	8.8	The ctl_report_supported_opcodes function did not sufficiently validate a field provided by userspace, allowing an arbitrary write	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a limited amount of kernel help memory. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host. **CVE ID: CVE-2024-42416**		
Out-of-bounds Read	05-Sep-2024	8.8	The ctl_request_sense function could expose up to three bytes of the kernel heap to userspace. Malicious software running in a guest VM that exposes virtio_scsi can	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3085

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
			exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host. **CVE ID: CVE-2024-43110**		
Use After Free	05-Sep-2024	8.8	The function ctl_write_buffer incorrectly set a flag which resulted in a kernel Use-After-Free when a command finished processing. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host. **CVE ID: CVE-2024-45063**		
Missing Initialization of Resource	05-Sep-2024	8.8	The ctl_write_buffer and ctl_read_buffer functions allocated memory to be returned to userspace, without initializing it. Malicious software running in a guest VM that exposes virtio_scsi can exploit the vulnerabilities to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the	https://security.freebsd.org/advisories/FreeBSD-SA-24:11.ctl.asc	O-FRE-FREE-190924/3087

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
			bhyve process. A malicious iSCSI initiator could achieve remote code execution on the iSCSI target host. **CVE ID: CVE-2024-8178**		
Out-of-bounds Write	05-Sep-2024	8.2	An insufficient boundary validation in the USB code could lead to an out-of-bounds write on the heap, with data controlled by the caller. A malicious, privileged software running in a guest VM can exploit the vulnerability to achieve code execution on the host in the bhyve userspace process, which typically runs as root. Note that bhyve runs in a Capsicum sandbox, so malicious code is constrained by the capabilities available to the bhyve process. **CVE ID: CVE-2024-32668**	https://security.freebsd.org/advisories/FreeBSD-SA-24:12.bhyve.asc	O-FRE-FREE-190924/3088
Integer Overflow or	05-Sep-2024	7.5	A malicious value of size in a structure of packed libnv can	https://security.freebsd.org/advisories/FreeBS	O-FRE-FREE-190924/3089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			cause an integer overflow, leading to the allocation of a smaller buffer than required for the parsed data. **CVE ID: CVE-2024-45287**	D-SA-24:09.libnv.asc	
Use After Free	05-Sep-2024	10	Concurrent removals of certain anonymous shared memory mappings by using the UMTX_SHM_DESTROY sub-request of UMTX_OP_SHM can lead to decreasing the reference count of the object representing the mapping too many times, causing it to be freed too early. A malicious code exercizing the UMTX_SHM_DESTROY sub-request in parallel can panic the kernel or enable further Use-After-Free attacks, potentially including code execution or Capsicum sandbox escape. **CVE ID: CVE-2024-43102**	https://security.freebsd.org/advisories/FreeBSD-SA-24:14.umtx.asc	O-FRE-FREE-190924/3090
Vendor: Google					
Product: android					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use After Free	11-Sep-2024	8.8	Use after free in Media Router in Google Chrome on Android prior to 128.0.6613.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-8637**	N/A	O-GOO-ANDR-190924/3091
Use After Free	11-Sep-2024	8.8	Use after free in Autofill in Google Chrome on Android prior to 128.0.6613.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-8639**	N/A	O-GOO-ANDR-190924/3092
N/A	03-Sep-2024	5.3	Multiple prompts and panels from both Firefox and the Android OS could be used to obscure the notification announcing the transition to fullscreen mode after the fix for	https://www.mozilla.org/security/advisories/mfsa2024-39/	O-GOO-ANDR-190924/3093

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
			CVE-2023-6870 in Firefox 121. This could lead to spoofing the browser UI if the sudden appearance of the prompt distracted the user from noticing the visual transition happening behind the prompt. These notifications now use the Android Toast feature. *This bug only affects Firefox on Android. Other operating systems are unaffected.* This vulnerability affects Firefox < 130. **CVE ID: CVE-2024-8388**		
Affected Version(s): 14.0					
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558;	https://corp.mediatek.com/product-security-bulletin/September-2024	O-GOO-ANDR-190924/3094

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
			Issue ID: MSV-1526. **CVE ID: CVE-2024-20089**		
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	O-GOO-ANDR-190924/3095
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	O-GOO-ANDR-190924/3096

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
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	O-GOO-ANDR-190924/3097
Affected Version(s): 12.0					
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1551. **CVE ID: CVE-2024-20086**	https://corp.mediatek.com/product-security-bulletin/September-2024	O-GOO-ANDR-190924/3098
Out-of-bounds Write	02-Sep-2024	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/September-2024	O-GOO-ANDR-190924/3099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932916; Issue ID: MSV-1550. **CVE ID: CVE-2024-20087**		
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	O-GOO-ANDR-190924/3100
Affected Version(s): 13.0					
Improper Check for Unusual or Exceptional Conditions	02-Sep-2024	7.5	In wlan, there is a possible denial of service due to incorrect error handling. This could lead to remote denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/September-2024	O-GOO-ANDR-190924/3101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08861558; Issue ID: MSV-1526. **CVE ID: CVE-2024-20089**		
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	O-GOO-ANDR-190924/3102
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204;	https://corp.mediatek.com/product-security-bulletin/September-2024	O-GOO-ANDR-190924/3103

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
			Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Out-of-bounds Read	02-Sep-2024	4.4	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08932099; Issue ID: MSV-1543. **CVE ID: CVE-2024-20088**	https://corp.mediatek.com/product-security-bulletin/September-2024	O-GOO-ANDR-190924/3104
Vendor: Huawei					
Product: emui					
Affected Version(s): 12.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Sep-2024	9.1	Directory traversal vulnerability in the cust module Impact: Successful exploitation of this vulnerability will affect availability and confidentiality. **CVE ID: CVE-2024-45443**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3105
N/A	04-Sep-2024	7.5	Access control vulnerability in the SystemUI module Impact: Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42039**		
N/A	04-Sep-2024	7.5	Input verification vulnerability in the system service module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45441**	https://https//consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3107
N/A	04-Sep-2024	7.5	Permission control vulnerability in the software update module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45450**	https://https//consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3108
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the WMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45444**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3109
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the	https://consumer.huawei.com/	O-HUA-EMUI-190924/3110

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
			camera driver module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45446**	en/support/bulletin/2024/9/	
N/A	04-Sep-2024	5.5	Access control vulnerability in the camera framework module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45447**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3111
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the ringtone setting module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45449**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3112
Affected Version(s): 13.0.0					
Improper Limitation of a Pathname to a Restricted Directory	04-Sep-2024	9.1	Directory traversal vulnerability in the cust module Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3113

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
('Path Traversal')			**CVE ID: CVE-2024-45443**		
N/A	04-Sep-2024	7.5	Access control vulnerability in the SystemUI module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42039**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3114
N/A	04-Sep-2024	7.5	Input verification vulnerability in the system service module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45441**	https://https//consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3115
N/A	04-Sep-2024	7.5	Vulnerability of permission verification for APIs in the DownloadProvider Main module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45442**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3116
N/A	04-Sep-2024	7.5	Permission control vulnerability in the software update module. Impact: Successful exploitation of this	https://https//consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3117

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
			vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45450**		
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the WMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45444**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3118
Incomplete Cleanup	04-Sep-2024	5.5	Vulnerability of resources not being closed or released in the keystore module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45445**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3119
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the camera driver module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45446**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3120
N/A	04-Sep-2024	5.5	Access control vulnerability in the	https://consumer.huawei.com/	O-HUA-EMUI-190924/3121

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
			camera framework module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45447**	en/support/bulletin/2024/9/	
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the ringtone setting module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45449**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3122
Affected Version(s): 14.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Sep-2024	9.1	Directory traversal vulnerability in the cust module Impact: Successful exploitation of this vulnerability will affect availability and confidentiality. **CVE ID: CVE-2024-45443**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3123
N/A	04-Sep-2024	7.5	Access control vulnerability in the SystemUI module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3124

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
			CVE ID: CVE-2024-42039		
N/A	04-Sep-2024	7.5	Input verification vulnerability in the system service module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45441**	https://https//consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3125
N/A	04-Sep-2024	7.5	Vulnerability of permission verification for APIs in the DownloadProvider Main module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45442**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3126
N/A	04-Sep-2024	7.5	Permission control vulnerability in the software update module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45450**	https://https//consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3127
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the WMS module	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3128

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
			Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45444**		
Incomplete Cleanup	04-Sep-2024	5.5	Vulnerability of resources not being closed or released in the keystore module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45445**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3129
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the camera driver module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45446**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3130
N/A	04-Sep-2024	5.5	Access control vulnerability in the camera framework module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45447**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3131

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
N/A	04-Sep-2024	5.5	Page table protection configuration vulnerability in the trusted firmware module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45448**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3132
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the ringtone setting module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45449**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3133
N/A	04-Sep-2024	5.5	Memory request vulnerability in the memory management module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-8298**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-EMUI-190924/3134
Product: harmonyos					
Affected Version(s): 2.0.0					

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
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Sep-2024	9.1	Directory traversal vulnerability in the cust module Impact: Successful exploitation of this vulnerability will affect availability and confidentiality. **CVE ID: CVE-2024-45443**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3135
N/A	04-Sep-2024	7.5	Access control vulnerability in the SystemUI module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42039**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3136
N/A	04-Sep-2024	7.5	Input verification vulnerability in the system service module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45441**	https://https//consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3137
N/A	04-Sep-2024	7.5	Permission control vulnerability in the software update module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	https://https//consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3138

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
			CVE ID: CVE-2024-45450		
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the WMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45444**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3139
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the camera driver module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45446**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3140
N/A	04-Sep-2024	5.5	Access control vulnerability in the camera framework module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45447**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3141
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the ringtone setting module	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3142

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
			Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45449**		
Affected Version(s): 2.1.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Sep-2024	9.1	Directory traversal vulnerability in the cust module Impact: Successful exploitation of this vulnerability will affect availability and confidentiality. **CVE ID: CVE-2024-45443**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3143
N/A	04-Sep-2024	7.5	Access control vulnerability in the SystemUI module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42039**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3144
N/A	04-Sep-2024	7.5	Input verification vulnerability in the system service module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45441**	https://https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3145
N/A	04-Sep-2024	7.5	Permission control vulnerability in the	https://https://consumer.huaw	O-HUA-HARM-190924/3146

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
			software update module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45450**	ei.com/en/support/bulletin/2024/9/	
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the WMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45444**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3147
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the camera driver module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45446**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3148
N/A	04-Sep-2024	5.5	Access control vulnerability in the camera framework module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3149

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
			CVE ID: CVE-2024-45447		
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the ringtone setting module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45449**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3150
Affected Version(s): 3.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Sep-2024	9.1	Directory traversal vulnerability in the cust module Impact: Successful exploitation of this vulnerability will affect availability and confidentiality. **CVE ID: CVE-2024-45443**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3151
N/A	04-Sep-2024	7.5	Access control vulnerability in the SystemUI module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42039**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3152
N/A	04-Sep-2024	7.5	Input verification vulnerability in the system service module	https://https//consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3153

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
			Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45441**		
N/A	04-Sep-2024	7.5	Permission control vulnerability in the software update module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45450**	https://https//consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3154
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the WMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45444**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3155
Incomplete Cleanup	04-Sep-2024	5.5	Vulnerability of resources not being closed or released in the keystore module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45445**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3156

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
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the camera driver module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45446**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3157
N/A	04-Sep-2024	5.5	Access control vulnerability in the camera framework module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45447**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3158
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the ringtone setting module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45449**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3159
Affected Version(s): 3.1.0					
Improper Limitation of a Pathname to a Restricted	04-Sep-2024	9.1	Directory traversal vulnerability in the cust module Impact: Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3160

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
Directory ('Path Traversal')			vulnerability will affect availability and confidentiality. **CVE ID: CVE-2024-45443**		
N/A	04-Sep-2024	7.5	Access control vulnerability in the SystemUI module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42039**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3161
N/A	04-Sep-2024	7.5	Input verification vulnerability in the system service module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45441**	https://https//consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3162
N/A	04-Sep-2024	7.5	Vulnerability of permission verification for APIs in the DownloadProviderMain module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45442**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3163
N/A	04-Sep-2024	7.5	Permission control vulnerability in the	https://https//consumer.huawei.com/en/supp	O-HUA-HARM-190924/3164

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
			software update module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45450**	ort/bulletin/2024/9/	
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the WMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45444**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3165
Incomplete Cleanup	04-Sep-2024	5.5	Vulnerability of resources not being closed or released in the keystore module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45445**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3166
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the camera driver module Impact: Successful exploitation of this vulnerability will affect availability.	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45446		
N/A	04-Sep-2024	5.5	Access control vulnerability in the camera framework module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45447**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3168
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the ringtone setting module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45449**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3169
Affected Version(s): 4.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Sep-2024	9.1	Directory traversal vulnerability in the cust module Impact: Successful exploitation of this vulnerability will affect availability and confidentiality. **CVE ID: CVE-2024-45443**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3170
N/A	04-Sep-2024	7.5	Access control vulnerability in the SystemUI module	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3171

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
			Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42039**		
N/A	04-Sep-2024	7.5	Input verification vulnerability in the system service module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45441**	https://https//consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3172
N/A	04-Sep-2024	7.5	Vulnerability of permission verification for APIs in the DownloadProviderMain module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45442**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3173
N/A	04-Sep-2024	7.5	Permission control vulnerability in the software update module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45450**	https://https//consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3174

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
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the WMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45444**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3175
Incomplete Cleanup	04-Sep-2024	5.5	Vulnerability of resources not being closed or released in the keystore module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45445**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3176
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the camera driver module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45446**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3177
N/A	04-Sep-2024	5.5	Access control vulnerability in the camera framework module Impact: Successful exploitation of this vulnerability may	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3178

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
			affect service confidentiality. **CVE ID: CVE-2024-45447**		
N/A	04-Sep-2024	5.5	Page table protection configuration vulnerability in the trusted firmware module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45448**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3179
N/A	04-Sep-2024	5.5	Memory request vulnerability in the memory management module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-8298**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3180
Affected Version(s): 4.2.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Sep-2024	9.1	Directory traversal vulnerability in the cust module Impact: Successful exploitation of this vulnerability will affect availability and confidentiality. **CVE ID: CVE-2024-45443**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3181

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
N/A	04-Sep-2024	7.5	Access control vulnerability in the SystemUI module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-42039**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3182
N/A	04-Sep-2024	7.5	Input verification vulnerability in the system service module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45441**	https://https//consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3183
N/A	04-Sep-2024	7.5	Vulnerability of permission verification for APIs in the DownloadProvider Main module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45442**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3184
N/A	04-Sep-2024	7.5	Permission control vulnerability in the software update module. Impact: Successful exploitation of this vulnerability may	https://https//consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3185

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
			affect service confidentiality. **CVE ID: CVE-2024-45450**		
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the WMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45444**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3186
Incomplete Cleanup	04-Sep-2024	5.5	Vulnerability of resources not being closed or released in the keystore module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45445**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3187
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the camera driver module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-45446**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3188
N/A	04-Sep-2024	5.5	Access control vulnerability in the	https://consumer.huawei.com/	O-HUA-HARM-190924/3189

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
			camera framework module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45447**	en/support/bulletin/2024/9/	
N/A	04-Sep-2024	5.5	Page table protection configuration vulnerability in the trusted firmware module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45448**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3190
N/A	04-Sep-2024	5.5	Access permission verification vulnerability in the ringtone setting module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-45449**	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3191
N/A	04-Sep-2024	5.5	Memory request vulnerability in the memory management module Impact: Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin/2024/9/	O-HUA-HARM-190924/3192

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
			vulnerability may affect service confidentiality. **CVE ID: CVE-2024-8298**		
Vendor: kasdanet					
Product: kw5515_firmware					
Affected Version(s): 4.3.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Sep-2024	4.3	Cross Site Scripting (XSS) Vulnerability in Firewall menu in Control Panel in KASDA KW5515 version 4.3.1.0, allows attackers to execute arbitrary code and steal cookies via a crafted script **CVE ID: CVE-2020-24061**	N/A	O-KAS-KW55-190924/3193
Vendor: Linksys					
Product: wrt54g_firmware					
Affected Version(s): 4.21.5					
Out-of-bounds Write	04-Sep-2024	9.8	A vulnerability was found in Linksys WRT54G 4.21.5. It has been rated as critical. Affected by this issue is the function validate_services_port of the file /apply.cgi of the component POST Parameter Handler. The manipulation of the argument services_array leads to stack-	N/A	O-LIN-WRT5-190924/3194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based buffer overflow. 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-2024-8408**		
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): * Up to (excluding) 4.14.326					
NULL Pointer Dereference	06-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: media: dvb-usb-v2: af9035: Fix null-ptr-deref in af9035_i2c_master_xfer In af9035_i2c_master_xfer, msg is controlled by user. When msg[i].buf is null and msg[i].len is zero, former checks on msg[i].buf would be	https://git.kernel.org/stable/c/0143f282b15f7cedc0392ea10050fb6000fd16e6, https://git.kernel.org/stable/c/41b7181a40af84448a2b144fb02d8bf32b7e9a23, https://git.kernel.org/stable/c/6c01ef65de0b321b2db1ef9abf8f1d15862b937e	O-LIN-LINU-190924/3195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed. Malicious data finally reach af9035_i2c_master_xfer. If accessing msg[i].buf[0] without sanity check, null ptr deref would happen. We add check on msg[i].len to prevent crash. Similar commit: commit 0ed554fd769a ("media: dvb-usb: az6027: fix null-ptr-deref in az6027_i2c_xfer()") **CVE ID: CVE-2023-52915**		
Affected Version(s): * Up to (excluding) 4.19.321					
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fix bitmap corruption on close_range() with CLOSE_RANGE_UNSHARE copy_fd_bitmaps(new, old, count) is expected to copy the first	https://git.kernel.org/stable/c/5053581fe5dfb09b58c65dd8462bf5dea71f41ff, https://git.kernel.org/stable/c/8cad3b2b3ab81ca55f37405ffd1315bcc2948058, https://git.kernel.org/stable/c/9a2fa1472083580b6c66bdaf291f591e1170123a	O-LIN-LINU-190924/3196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			count/BITS_PER_LONG bits from old->full_fds_bits[] and fill the rest with zeroes. What it does is copying enough words (BITS_TO_LONGS(count/BITS_PER_LONG)), then memsets the rest. That works fine, *if* all bits past the cutoff point are clear. Otherwise we are risking garbage from the last word we'd copied. For most of the callers that is true - expand_fdtable() has count equal to old->max_fds, so there's no open descriptors past count, let alone fully occupied words in ->open_fds[], which is what bits in ->full_fds_bits[] correspond to. The other caller (dup_fd()) passes		

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
			sane_fdtable_size(old_fdt, max_fds), which is the smallest multiple of BITS_PER_LONG that covers all opened descriptors below max_fds. In the common case (copying on fork()) max_fds is ~0U, so all opened descriptors will be below it and we are fine, by the same reasons why the call in expand_fdtable() is safe. Unfortunately, there is a case where max_fds is less than that and where we might, indeed, end up with junk in ->full_fds_bits[] - close_range(from, to, CLOSE_RANGE_UNSHARE) with * descriptor table being currently shared * 'to' being above the current capacity of descriptor table		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 'from' being just under some chunk of opened descriptors. In that case we end up with observably wrong behaviour - e.g. spawn a child with CLONE_FILES, get all descriptors in range 0..127 open, then close_range(64, ~0U, CLOSE_RANGE_UNSHARE) and watch dup(0) ending up with descriptor #128, despite #64 being observably not open. The minimally invasive fix would be to deal with that in dup_fd(). If this proves to add measurable overhead, we can go that way, but let's try to fix copy_fd_bitmaps() first. * new helper: bitmap_copy_and_expand(to, from, bits_to_copy, size).		

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
			* make copy_fd_bitmaps() take the bitmap size in words, rather than bits; it's 'count' argument is always a multiple of BITS_PER_LONG, so we are not losing any information, and that way we can use the same helper for all three bitmaps - compiler will see that count is a multiple of BITS_PER_LONG for the large ones, so it'll generate plain memcpy()+memset(). Reproducer added to tools/testing/selftests/core/close_range_test.c **CVE ID: CVE-2024-45025**		
Affected Version(s): * Up to (excluding) 6.10.5					
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/xe/preempt_fence: enlarge the	https://git.kernel.org/stable/c/3cd1585e57908b6efcd967465ef7685f40b2a294, https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fence critical section It is really easy to introduce subtle deadlocks in preempt_fence_work_func() since we operate on single global ordered-wq for signalling our preempt fences behind the scenes, so even though we signal a particular fence, everything in the callback should be in the fence critical section, since blocking in the callback will prevent other published fences from signalling. If we enlarge the fence critical section to cover the entire callback, then lockdep should be able to understand this better, and complain if we grab a sensitive lock like vm->lock, which is also held when waiting on preempt fences.	458bb83119dfee5d14c677f7846dd9363817006f	

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
			CVE ID: CVE-2024-44956		
Affected Version(s): * Up to (excluding) 6.10.8					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/mes: fix mes ring buffer overflow wait memory room until enough before writing mes packets to avoid ring buffer overflow. v2: squash in sched_hw_submission fix (cherry picked from commit 34e087e8920e635c62e2ed6a758b0cd27f836d13) **CVE ID: CVE-2024-46700**	https://git.kernel.org/stable/c/11752c013f562a1124088a35bd314aa0e9f0e88f, https://git.kernel.org/stable/c/ed37550d7c516017c3b0324bdf144e2fa563ffb0	O-LIN-LINU-190924/3198
Affected Version(s): * Up to (excluding) 6.6.46					
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: xen: privcmd: Switch from mutex	https://git.kernel.org/stable/c/1c682593096a487fd9aebc079a307ff7a6d054a3, https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to spinlock for irqfds irqfd_wakeup() gets EPOLLHUP, when it is called by eventfd_release() by way of wake_up_poll(&ctx->wqh, EPOLLHUP), which gets called under spin_lock_irqsave(). We can't use a mutex here as it will lead to a deadlock. Fix it by switching over to a spin lock. **CVE ID: CVE-2024-44957**	49f2a5da6785b2dbde93e291cae037662440346e, https://git.kernel.org/stable/c/c2775ae4d9227729f8ca9ee2a068f62a00d5ea9c	
Affected Version(s): 6.11					
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: mtk_wed: fix use-after-free panic in mtk_wed_setup_tc_block_cb() When there are multiple ap interfaces on one band and with WED on,	https://git.kernel.org/stable/c/326a89321f9d5fe399fe6f9ff7c0fc766582a6a0, https://git.kernel.org/stable/c/b453a4bbda03aa8741279c360ac82d1c3ac33548, https://git.kernel.org/stable/c/db1b4bedb9b97c6d34b03d03815147c04fffe8b4	O-LIN-LINU-190924/3200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			turning the interface down will cause a kernel panic on MT798X. Previously, cb_priv was freed in mtk_wed_setup_tc_block() without marking NULL,and mtk_wed_setup_tc_block_cb() didn't check the value, too. Assign NULL after free cb_priv in mtk_wed_setup_tc_block() and check NULL in mtk_wed_setup_tc_block_cb(). ---------- Unable to handle kernel paging request at virtual address 0072460bca32b4f5 Call trace: mtk_wed_setup_tc_block_cb+0x4/0x38 0xffffffc0794084bc tcf_block_playback_		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			offloads+0x70/0x1e8 tcf_block_unbind+0x6c/0xc8 ... --------- **CVE ID: CVE-2024-44997**		
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: atm: idt77252: prevent use after free in dequeue_rx() We can't dereference "skb" after calling vcc->push() because the skb is released. **CVE ID: CVE-2024-44998**	https://git.kernel.org/stable/c/09e086a5f72ea27c758b3f3b419a69000c32adc1, https://git.kernel.org/stable/c/1cece837e387c039225f19028df255df87a97c0d, https://git.kernel.org/stable/c/24cf390a5426aac9255205e9533cdd7b4235d518	O-LIN-LINU-190924/3201
Missing Release of Memory after Effective Lifetime	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: idpf: fix memory leaks and crashes while performing a soft reset The second tagged commit introduced	https://git.kernel.org/stable/c/6b289f8d91537ec1e4f9c7b38b31b90d93b1419b, https://git.kernel.org/stable/c/f01032a2ca099ec8d619aaa916c3762aa62495df	O-LIN-LINU-190924/3202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a UAF, as it removed restoring q_vector->vport pointers after reinitializating the structures. This is due to that all queue allocation functions are performed here with the new temporary vport structure and those functions rewrite the backpointers to the vport. Then, this new struct is freed and the pointers start leading to nowhere. But generally speaking, the current logic is very fragile. It claims to be more reliable when the system is low on memory, but in fact, it consumes two times more memory as at the moment of running this function, there are two vports allocated with their queues and vectors. Moreover, it claims to prevent the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			driver from running into "bad state", but in fact, any error during the rebuild leaves the old vport in the partially allocated state. Finally, if the interface is down when the function is called, it always allocates a new queue set, but when the user decides to enable the interface later on, vport_open() allocates them once again, IOW there's a clear memory leak here. Just don't allocate a new queue set when performing a reset, that solves crashes and memory leaks. Readd the old queue number and reopen the interface on rollback - that solves limbo states when the device is left		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disabled and/or without HW queues enabled. **CVE ID: CVE-2024-44964**		
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: avoid possible UaF when selecting endp select_local_address() and select_signal_address() both select an endpoint entry from the list inside an RCU protected section, but return a reference to it, to be read later on. If the entry is dereferenced after the RCU unlock, reading info could cause a Use-after-Free. A simple solution is to copy the required info while inside the RCU protected section to avoid any risk of UaF later. The address ID might	https://git.kernel.org/stable/c/0201d65d9806d287a00e0ba96f0321835631f63f, https://git.kernel.org/stable/c/48e50dcbcbaaf713d82bf2da5c16aeced94ad07d, https://git.kernel.org/stable/c/9a9afbbc3fbfca4975eea4aa5b18556db5a0c0b8	O-LIN-LINU-190924/3203

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
			need to be modified later to handle the ID0 case later, so a copy seems OK to deal with. **CVE ID: CVE-2024-44974**		
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Free job before xe_exec_queue_put Free job depends on job->vm being valid, the last xe_exec_queue_put can destroy the VM. Prevent UAF by freeing job before xe_exec_queue_put. (cherry picked from commit 32a42c93b74c8ca6d0915ea3eba21bceff53042f) **CVE ID: CVE-2024-44978**	https://git.kernel.org/stable/c/98aa0330f200b9b8fb9e1298e006eda57a13351c, https://git.kernel.org/stable/c/9e7f30563677fbeff62d368d5d2a5ac7aaa9746a	O-LIN-LINU-190924/3204
Double Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/10d9d8c3512f16cad47b2ff81ec6fc4b27d8ee10, https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			btrfs: fix a use-after-free when hitting errors inside btrfs_submit_chunk() [BUG] There is an internal report that KASAN is reporting use-after-free, with the following backtrace: BUG: KASAN: slab-use-after-free in btrfs_check_read_bio+0xa68/0xb70 [btrfs] Read of size 4 at addr ffff8881117cec28 by task kworker/u16:2/45 CPU: 1 UID: 0 PID: 45 Comm: kworker/u16:2 Not tainted 6.11.0-rc2-next-20240805-default+ #76 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.2-3-gd478f380-rebuilt.opensuse.org 04/01/2014 Workqueue: btrfs-endio	4a3b9e1a8e6cd1a8d427a905e159de58d38941cc, https://git.kernel.org/stable/c/51722b99f41f5e722ffa10b8f61e802a0e70b331	

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
			btrfs_end_bio_work [btrfs] Call Trace: dump_stack_lvl+0x61/0x80 print_address_description.constprop.0+0x5e/0x2f0 print_report+0x118/0x216 kasan_report+0x11d/0x1f0 btrfs_check_read_bio+0xa68/0xb70 [btrfs] process_one_work+0xce0/0x12a0 worker_thread+0x717/0x1250 kthread+0x2e3/0x3c0 ret_from_fork+0x2d/0x70 ret_from_fork_asm+0x11/0x20 Allocated by task 20917:		

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
			kasan_save_stack+0x37/0x60 kasan_save_track+0x10/0x30 __kasan_slab_alloc+0x7d/0x80 kmem_cache_alloc_noprof+0x16e/0x3e0 mempool_alloc_noprof+0x12e/0x310 bio_alloc_bioset+0x3f0/0x7a0 btrfs_bio_alloc+0x2e/0x50 [btrfs] submit_extent_page+0x4d1/0xdb0 [btrfs] btrfs_do_readpage+0x8b4/0x12a0 [btrfs] btrfs_readahead+0x29a/0x430 [btrfs] read_pages+0x1a7/0xc60 page_cache_ra_unbounded+0x2ad/0x560		

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
			filemap_get_pages+0x629/0xa20 filemap_read+0x335/0xbf0 vfs_read+0x790/0xcb0 ksys_read+0xfd/0x1d0 do_syscall_64+0x6d/0x140 entry_SYSCALL_64_after_hwframe+0x4b/0x53 Freed by task 20917: kasan_save_stack+0x37/0x60 kasan_save_track+0x10/0x30 kasan_save_free_info+0x37/0x50 __kasan_slab_free+0x4b/0x60 kmem_cache_free+0x214/0x5d0		

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
			bio_free+0xed/0x180 end_bbio_data_read+0x1cc/0x580 [btrfs] btrfs_submit_chunk+0x98d/0x1880 [btrfs] btrfs_submit_bio+0x33/0x70 [btrfs] submit_one_bio+0xd4/0x130 [btrfs] submit_extent_page+0x3ea/0xdb0 [btrfs] btrfs_do_readpage+0x8b4/0x12a0 [btrfs] btrfs_readahead+0x29a/0x430 [btrfs] read_pages+0x1a7/0xc60 page_cache_ra_unbounded+0x2ad/0x560 filemap_get_pages+0x629/0xa20		

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
			filemap_read+0x335/0xbf0 vfs_read+0x790/0xcb0 ksys_read+0xfd/0x1d0 do_syscall_64+0x6d/0x140 entry_SYSCALL_64_after_hwframe+0x4b/0x53 [CAUSE] Although I cannot reproduce the error, the report itself is good enough to pin down the cause. The call trace is the regular endio workqueue context, but the free-by-task trace is showing that during btrfs_submit_chunk() we already hit a critical error, and is calling btrfs_bio_end_io() to error		

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
			out. And the original endio function called bio_put() to free the whole bio. This means a double freeing thus causing use-after-free, e.g.: 1. Enter btrfs_submit_bio() with a read bio The read bio length is 128K, crossing two 64K stripes. 2. The first run of btrfs_submit_chunk () 2.1 Call btrfs_map_block(), which returns 64K 2.2 Call btrfs_split_bio() Now there are two bios, one referring to the first 64K, the other referring to the second 64K. 2.3 The first half is submitted.		

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
			3. The second run of btrfs_submit_chunk () 3.1 Call btrfs_map_block(), which by somehow failed Now we call btrfs_bio_end_io() to handle the error 3.2 btrfs_bio_end_io() calls the original endio function Which is end_bbio_data_read(), and it calls bio_put() for the original bio. Now the original bio is freed. 4. The submitted first 64K bio finished Now we call into btrfs_check_read_bio() and tries to advance the bio iter. But since the original bio (thus its iter) is already freed, we		

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
			trigger the above use-after free. And even if the memory is not poisoned/corrupted, we will later call the original endio function, causing a double freeing. [FIX] Instead of calling btrfs_bio_end_io(), call btrfs_orig_bbio_end_io(), which has the extra check on split bios and do the pr ---truncated--- **CVE ID: CVE-2024-46687**		
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent possible UAF in ip6_xmit() If skb_expand_head() returns NULL, skb has been freed and the associated dst/idev could also have been freed.	https://git.kernel.org/stable/c/124b428fe28064c809e4237b0b38e97200a8a4a8, https://git.kernel.org/stable/c/2d5ff7e339d04622d8282661df36151906d0e1c7, https://git.kernel.org/stable/c/38a21c026ed2cc7232414cb166efc1923f34af17	O-LIN-LINU-190924/3206

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
			We must use rcu_read_lock() to prevent a possible UAF. **CVE ID: CVE-2024-44985**		
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: ipv6: fix possible UAF in ip6_finish_output2() If skb_expand_head() returns NULL, skb has been freed and associated dst/idev could also have been freed. We need to hold rcu_read_lock() to make sure the dst and associated idev are alive. **CVE ID: CVE-2024-44986**	https://git.kernel.org/stable/c/3574d28caf9a09756ae87ad1ea096c6f47b6101e, https://git.kernel.org/stable/c/56efc253196751ece1fc535a5b582be127b0578a, https://git.kernel.org/stable/c/6ab6bf731354a6fdbaa617d1ec194960db61cf3b	O-LIN-LINU-190924/3207
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/24e93695b1239fbe4c31e224372be77f82dab69a, https://git.kern	O-LIN-LINU-190924/3208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ipv6: prevent UAF in ip6_send_skb() syzbot reported an UAF in ip6_send_skb() [1] After ip6_local_out() has returned, we no longer can safely dereference rt, unless we hold rcu_read_lock(). A similar issue has been fixed in commit a688caa34beb ("ipv6: take rcu lock in rawv6_send_hdrinc()") Another potential issue in ip6_finish_output2() is handled in a separate patch. [1] BUG: KASAN: slab-use-after-free in ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 Read of size 8 at addr	el.org/stable/c/571567e0277008459750f0728f246086b2659429, https://git.kernel.org/stable/c/9a3e55afa95ed4ac9eda112d4f918af645d72f25	

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
			ffff88806dde4858 by task syz.1.380/6530 CPU: 1 UID: 0 PID: 6530 Comm: syz.1.380 Not tainted 6.11.0-rc3-syzkaller-00306-gdf6cbc62cc9b #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/06/2024 Call Trace: <TASK> __dump_stack lib/dump_stack.c:93 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:119 print_address_description mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x143/0x180		

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
			mm/kasan/report.c:601 ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 rawv6_push_pending_frames+0x75c/0x9e0 net/ipv6/raw.c:588 rawv6_sendmsg+0x19c7/0x23c0 net/ipv6/raw.c:926 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 sock_write_iter+0x2dd/0x400 net/socket.c:1160 do_iter_readv_writev+0x60a/0x890 vfs_writev+0x37c/0xbb0 fs/read_write.c:971 do_writev+0x1b1/0x350		

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
			fs/read_write.c:1018 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f936bf79e79 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 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 a8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f936cd7f038 EFLAGS: 00000246 ORIG_RAX: 0000000000000014 RAX: ffffffffffffffda RBX: 00007f936c115f80 RCX: 00007f936bf79e79 RDX: 0000000000000000		

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
			1 RSI: 0000000020000040 RDI: 0000000000000004 RBP: 00007f936bfe7916 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000000 R14: 00007f936c115f80 R15: 00007fff2860a7a8 </TASK> Allocated by task 6530: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 unpoison_slab_object		

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
			mm/kasan/common.c:312 [inline] __kasan_slab_alloc+0x66/0x80 mm/kasan/common.c:338 kasan_slab_alloc include/linux/kasan.h:201 [inline] slab_post_alloc_hook mm/slub.c:3988 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_noprof+0x135/0x2a0 mm/slub.c:4044 dst_alloc+0x12b/0x190 net/core/dst.c:89 ip6_blackhole_route+0x59/0x340 net/ipv6/route.c:2670 make_blackhole net/xfrm/xfrm_policy.c:3120 [inline] xfrm_lookup_route+0xd1/0x1c0 net/xfrm/xfrm_policy.c:3313 ip6_dst_lookup_flow+0x13e/0x180		

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
			net/ipv6/ip6_output.c:1257 rawv6_sendmsg+0x1283/0x23c0 net/ipv6/raw.c:898 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 ___sys_sendmsg+0x525/0x7d0 net/socket.c:2597 ___sys_sendmsg net/socket.c:2651 [inline] __sys_sendmsg+0x2b0/0x3a0 net/socket.c:2680 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 45:		

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
			kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 kasan_save_free_info+0x40/0x50 mm/kasan/generic.c:579 poison_slab_object+0xe0/0x150 mm/kasan/common.c:240 __kasan_slab_free+0x37/0x60 mm/kasan/common.c:256 kasan_slab_free include/linux/kasan.h:184 [inline] slab_free_hook mm/slub.c:2252 [inline] slab_free mm/slub.c:4473 [inline] kmem_cache_free+0x145/0x350 mm/slub.c:4548 dst_destroy+0x2ac/0x460 net/core/dst.c:124		

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
			rcu_do_batch kernel/rcu/tree.c:2569 [inline] rcu_core+0xafd/0x1830 kernel/rcu/tree. ---truncated--- **CVE ID: CVE-2024-44987**		
Out-of-bounds Write	11-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: s390/dasd: fix error recovery leading to data corruption on ESE devices Extent Space Efficient (ESE) or thin provisioned volumes need to be formatted on demand during usual IO processing. The dasd_ese_needs_format function checks for error codes that signal the non existence of a proper track format.	https://git.kernel.org/stable/c/0a228896a1b3654cd461ff654f6a64e97a9c3246, https://git.kernel.org/stable/c/19f60a55b2fda49bc4f6134a5f6356ef62ee69d8, https://git.kernel.org/stable/c/5d4a304338daf83ace2887aaacafd66fe99ed5cc	O-LIN-LINU-190924/3209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The check for incorrect length is to imprecise since other error cases leading to transport of insufficient data also have this flag set. This might lead to data corruption in certain error cases for example during a storage server warmstart. Fix by removing the check for incorrect length and replacing by explicitly checking for invalid track format in transport mode. Also remove the check for file protected since this is not a valid ESE handling case. **CVE ID: CVE-2024-45026**		
Double Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/4b540ec7c0045c2d01c4e479f34bbc8f147afa4c, https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scsi: aacraid: Fix double-free on probe failure aac_probe_one() calls hardware-specific init functions through the aac_driver_ident::init pointer, all of which eventually call down to aac_init_adapter(). If aac_init_adapter() fails after allocating memory for aac_dev::queues, it frees the memory but does not clear that member. After the hardware-specific init function returns an error, aac_probe_one() goes down an error path that frees the memory pointed to by aac_dev::queues, resulting.in a double-free. **CVE ID: CVE-2024-46673**	564e1986b00c5f05d75342f8407f75f0a17b94df, https://git.kernel.org/stable/c/60962c3d8e18e5d8dfa16df788974dd7f35bd87a	
Use After Free	13-Sep-2024	7.8	In the Linux kernel, the following	https://git.kernel.org/stable/c/060f41243ad7f	O-LIN-LINU-190924/3211

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
			vulnerability has been resolved: usb: dwc3: st: fix probed platform device ref count on probe error path The probe function never performs any paltform device allocation, thus error path "undo_platform_dev_alloc" is entirely bogus. It drops the reference count from the platform device being probed. If error path is triggered, this will lead to unbalanced device reference counts and premature release of device resources, thus possible use-after-free when releasing remaining devm-managed resources. **CVE ID: CVE-2024-46674**	6f5249fa7290dda0c01f723d12d, https://git.kernel.org/stable/c/1de989668708ce5875efc9d669d227212aeb9a90, https://git.kernel.org/stable/c/4c6735299540f3c82a5033d35be76a5c42e0fb18	
Use After Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/10081b0b0ed201f53e24bd92deb2e0f3c3e713	O-LIN-LINU-190924/3212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drm/xe: prevent UAF around preempt fence The fence lock is part of the queue, therefore in the current design anything locking the fence should then also hold a ref to the queue to prevent the queue from being freed. However, currently it looks like we signal the fence and then drop the queue ref, but if something is waiting on the fence, the waiter is kicked to wake up at some later point, where upon waking up it first grabs the lock before checking the fence state. But if we have already dropped the queue ref, then the lock might already be freed as part of the queue, leading to uaf. To prevent this, move the fence lock	d4, https://git.kernel.org/stable/c/730b72480e29f63fd644f5fa57c9d46109428953	

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
			into the fence itself so we don't run into lifetime issues. Alternative might be to have device level lock, or only release the queue in the fence release callback, however that might require pushing to another worker to avoid locking issues. References: https://gitlab.freedesktop.org/drm/xe/kernel/-/issues/2454 References: https://gitlab.freedesktop.org/drm/xe/kernel/-/issues/2342 References: https://gitlab.freedesktop.org/drm/xe/kernel/-/issues/2020 (cherry picked from commit 7116c35aacedc38be6d15bd21b2fc936eed0008b) **CVE ID: CVE-2024-46683**		
Use After Free	13-Sep-2024	7.8	In the Linux kernel, the following	https://git.kernel.org/stable/c/1116e0e372eb16dd907ec571ce	O-LIN-LINU-190924/3213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: nfsd: fix potential UAF in nfsd4_cb_getattr_release Once we drop the delegation reference, the fields embedded in it are no longer safe to access. Do that last. **CVE ID: CVE-2024-46696**	5d4af325c55c10, https://git.kernel.org/stable/c/e0b66698a5ae41078f7490e8b3527013f5fccd6c	
N/A	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Disable preemption while updating GPU stats We forgot to disable preemption around the write_seqcount_begin/end() pair while updating GPU stats: [ ] WARNING: CPU: 2 PID: 12 at include/linux/seqlock.h:221 __seqprop_assert.is	https://git.kernel.org/stable/c/1e93467ef20308da5a94cde548ee17d523e8ba7b, https://git.kernel.org/stable/c/9d824c7fce58f59982228aa85b0376b113cdfa35	O-LIN-LINU-190924/3214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ra.0+0x128/0x150 [v3d] [ ] Workqueue: v3d_bin drm_sched_run_job _work [gpu_sched] <...snip...> [ ] Call trace: [ ] __seqprop_assert.is ra.0+0x128/0x150 [v3d] [ ] v3d_job_start_stats. isra.0+0x90/0x218 [v3d] [ ] v3d_bin_job_run+0 x23c/0x388 [v3d] [ ] drm_sched_run_job _work+0x520/0x6 d0 [gpu_sched] [ ] process_one_work +0x62c/0xb48 [ ] worker_thread+0x 468/0x5b0 [ ] kthread+0x1c4/0x 1e0 [ ] ret_from_fork+0x1 0/0x20 Fix it. **CVE ID: CVE-2024-46699**		

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 Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/mes: fix mes ring buffer overflow wait memory room until enough before writing mes packets to avoid ring buffer overflow. v2: squash in sched_hw_submission fix (cherry picked from commit 34e087e8920e635c62e2ed6a758b0cd27f836d13) **CVE ID: CVE-2024-46700**	https://git.kernel.org/stable/c/11752c013f562a1124088a35bd314aa0e9f0e88f, https://git.kernel.org/stable/c/ed37550d7c516017c3b0324bdf144e2fa563ffb0	O-LIN-LINU-190924/3215
Out-of-bounds Read	04-Sep-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Fix out-of-bounds read in `v3d_csd_job_run()` When enabling UBSAN on Raspberry Pi 5, we	https://git.kernel.org/stable/c/497d370a644d95a9f04271aa92cb96d32e84c770, https://git.kernel.org/stable/c/d656b82c4b30cf12715e6cd129d3df808fde24a7	O-LIN-LINU-190924/3216

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
			get the following warning: [387.894977] UBSAN: array-index-out-of-bounds in drivers/gpu/drm/v3d/v3d_sched.c:320:3 [387.903868] index 7 is out of range for type '__u32 [7]' [387.909692] CPU: 0 PID: 1207 Comm: kworker/u16:2 Tainted: G WC 6.10.3-v8-16k-numa #151 [387.919166] Hardware name: Raspberry Pi 5 Model B Rev 1.0 (DT) [387.925961] Workqueue: v3d_csd drm_sched_run_job_work [gpu_sched] [387.932525] Call trace: [387.935296] dump_backtrace+0x170/0x1b8 [387.939403] show_stack+0x20/0x38		

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
			[387.942907] dump_stack_lvl+0x90/0xd0 [387.946785] dump_stack+0x18/0x28 [387.950301] __ubsan_handle_out_of_bounds+0x98/0xd0 [387.955383] v3d_csd_job_run+0x3a8/0x438 [v3d] [387.960707] drm_sched_run_job_work+0x520/0x6d0 [gpu_sched] [387.966862] process_one_work+0x62c/0xb48 [387.971296] worker_thread+0x468/0x5b0 [387.975317] kthread+0x1c4/0x1e0 [387.978818] ret_from_fork+0x10/0x20 [387.983014] ---[end trace]--- This happens because the UAPI provides only seven configuration registers and we are reading the		

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
			eighth position of this u32 array. Therefore, fix the out-of-bounds read in `v3d_csd_job_run()` by accessing only seven positions on the '__u32 [7]' array. The eighth register exists indeed on V3D 7.1, but it isn't currently used. That being so, let's guarantee that it remains unused and add a note that it could be set in a future patch. **CVE ID: CVE-2024-44993**		
Use of Uninitialized Resource	04-Sep-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: gtp: pull network headers in gtp_dev_xmit() syzbot/KMSAN reported use of uninit-value in get_dev_xmit() [1]	https://git.kernel.org/stable/c/137d565ab89ce3584503b443bc9e00d44f482593, https://git.kernel.org/stable/c/1f6b62392453d8f36685d19b761307a8c5617ac1, https://git.kernel.org/stable/c/34ba4f29f3d9eb52dee375120	O-LIN-LINU-190924/3217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			We must make sure the IPv4 or Ipv6 header is pulled in skb->head before accessing fields in them. Use pskb_inet_may_pull() to fix this issue. [1] BUG: KMSAN: uninit-value in ipv6_pdp_find drivers/net/gtp.c:220 [inline] BUG: KMSAN: uninit-value in gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] BUG: KMSAN: uninit-value in gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281 ipv6_pdp_find drivers/net/gtp.c:220 [inline] gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281	59efb2afd7e966f	

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
			__netdev_start_xmit include/linux/netdevice.h:4913 [inline] netdev_start_xmit include/linux/netdevice.h:4922 [inline] xmit_one net/core/dev.c:3580 [inline] dev_hard_start_xmit+0x247/0xa20 net/core/dev.c:3596 __dev_queue_xmit+0x358c/0x5610 net/core/dev.c:4423 dev_queue_xmit include/linux/netdevice.h:3105 [inline] packet_xmit+0x9c/0x6c0 net/packet/af_packet.c:276 packet_snd net/packet/af_packet.c:3145 [inline] packet_sendmsg+0x90e3/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nos		

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
			ec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f		

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
			Uninit was created at: slab_post_alloc_hook mm/slub.c:3994 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_node_noprof+0x6bf/0xb80 mm/slub.c:4080 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:583 __alloc_skb+0x363/0x7b0 net/core/skbuff.c:674 alloc_skb include/linux/skbuff.h:1320 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6526 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2815 packet_alloc_skb net/packet/af_packet.c:2994 [inline]		

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
			packet_snd net/packet/af_packet.c:3088 [inline] packet_sendmsg+0x749c/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd		

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
			/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f CPU: 0 UID: 0 PID: 7115 Comm: syz.1.515 Not tainted 6.11.0-rc1-syzkaller-00043-g94ede2a3e913 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 **CVE ID: CVE-2024-44999**		
Use of Uninitialized Resource	04-Sep-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: validate vlan header Ensure there is sufficient room to access the protocol field of the VLAN header, validate it once before the flowtable lookup.	https://git.kernel.org/stable/c/0279c35d242d037abeb73d60d06a6d1bb7f672d9, https://git.kernel.org/stable/c/043a18bb6cf16adaa2f8642acfde6e8956a9caaa, https://git.kernel.org/stable/c/6ea14ccb60c8ab829349979b22b58a941ec4a3ee	O-LIN-LINU-190924/3218

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
			========== ========== ========== ======== BUG: KMSAN: uninit-value in nf_flow_offload_inet_hook+0x45a/0x5f0 net/netfilter/nf_flow_table_inet.c:32 nf_flow_offload_inet_hook+0x45a/0x5f0 net/netfilter/nf_flow_table_inet.c:32 nf_hook_entry_hookfn include/linux/netfilter.h:154 [inline] nf_hook_slow+0xf4/0x400 net/netfilter/core.c:626 nf_hook_ingress include/linux/netfilter_netdev.h:34 [inline] nf_ingress net/core/dev.c:5440 [inline] **CVE ID: CVE-2024-44983**		
Out-of-bounds Write	11-Sep-2024	7.1	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/2febf5fdbf5d9a52ddc3e98697	O-LIN-LINU-190924/3219

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

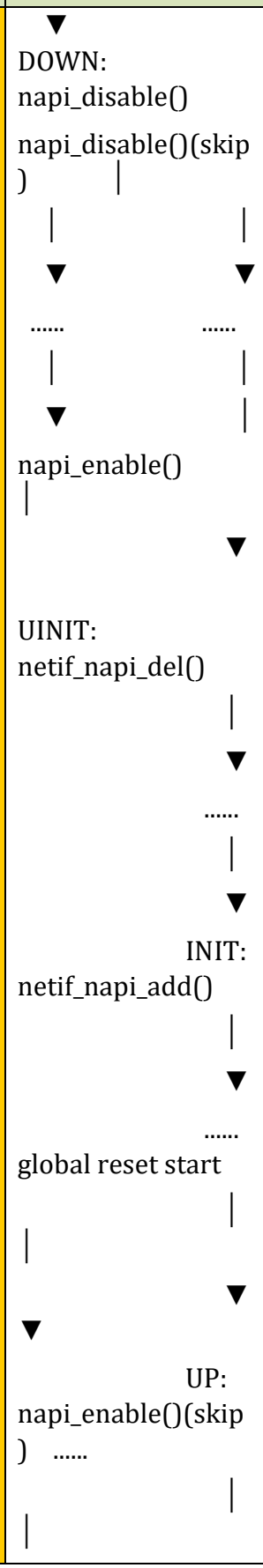
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			md/raid1: Fix data corruption for degraded array with slow disk read_balance() will avoid reading from slow disks as much as possible, however, if valid data only lands in slow disks, and a new normal disk is still in recovery, unrecovered data can be read: raid1_read_request read_balance raid1_should_read_first -> return false choose_best_rdev -> normal disk is not recovered, return -1 choose_bb_rdev -> missing the checking of recovery, return the normal disk -> read unrecovered data Root cause is that the checking of	1c8609b1582d67, https://git.kernel.org/stable/c/c916ca35308d3187c9928664f9be249b22a3a701	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recovery is missing in choose_bb_rdev(). Hence add such checking to fix the problem. Also fix similar problem in choose_slow_rdev( ). **CVE ID: CVE-2024-45023**		
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix a deadlock problem when config TC during resetting When config TC during the reset process, may cause a deadlock, the flow is as below: pf reset start | ▼ ..... setup tc | | ▼	https://git.kernel.org/stable/c/195918217448a6bb7f929d6a2ffffce9f1ece1cc, https://git.kernel.org/stable/c/67492d4d105c0a6321b00c393eec96b9a7a97a16, https://git.kernel.org/stable/c/6ae2b7d63cd056f363045eb65409143e16f23ae8	O-LIN-LINU-190924/3220

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
					

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
			▼ ▼ ..... napi_disable() In reset process, the driver will DOWN the port and then UINIT, in this case, the setup tc process will UP the port before UINIT, so cause the problem. Adds a DOWN process in UINIT to fix it. **CVE ID: CVE-2024-44995**		
Uncontrolled Recursion	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: vsock: fix recursive ->recvmsg calls After a vsock socket has been added to a BPF sockmap, its prot->recvmsg has been replaced with vsock_bpf_recvmsg (). Thus the following recursiion could happen:	https://git.kernel.org/stable/c/69139d2919dd4aa9a553c8245e7c63e82613e3fc, https://git.kernel.org/stable/c/921f1acf0c3cf6b1260ab57a8a6e8b3d5f3023d5, https://git.kernel.org/stable/c/b4ee8cf1acc5018ed1369150d7bb3e0d0f79e135	O-LIN-LINU-190924/3221

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_bpf_recvmsg () -> __vsock_recvmsg() -> vsock_connectible_recvmsg() -> prot->recvmsg() -> vsock_bpf_recvmsg() again We need to fix it by calling the original ->recvmsg() without any BPF sockmap logic in __vsock_recvmsg(). **CVE ID: CVE-2024-44996**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fs/netfs/fscache_cookie: add missing "n_accesses" check This fixes a NULL pointer dereference bug due to a data race which looks like this: BUG: kernel NULL pointer	https://git.kernel.org/stable/c/0a4d41fa14b2a0efd40e350cfe8ec6a4c998ac1d, https://git.kernel.org/stable/c/b8a50877f68efdcc0be3fcc5116e00c31b90e45b, https://git.kernel.org/stable/c/dfaa39b05a6cf34a16c525a2759ee6ab26b5fef6	O-LIN-LINU-190924/3222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dereference, address: 0000000000000008 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] SMP PTI CPU: 33 PID: 16573 Comm: kworker/u97:799 Not tainted 6.8.7-cm4all1-hp+ #43 Hardware name: HP ProLiant DL380 Gen9/ProLiant DL380 Gen9, BIOS P89 10/17/2018 Workqueue: events_unbound netfs_rreq_write_to_cache_work RIP: 0010:cachefiles_prepare_write+0x30/0xa0 Code: 57 41 56 45 89 ce 41 55 49 89 cd 41 54 49 89 d4 55 53 48 89 fb 48 83 ec 08 48 8b 47 08 48 83 7f 10 00 48 89 34 24 48 8b 68 20 <48> 8b 45 08 4c 8b 38 74 45		

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
			49 8b 7f 50 e8 4e a9 b0 ff 48 8b 73 10 RSP: 0018:ffffb4e78113bde0 EFLAGS: 00010286 RAX: ffff976126be6d10 RBX: ffff97615cdb8438 RCX: 0000000000020000 RDX: ffff97605e6c4c68 RSI: ffff97605e6c4c60 RDI: ffff97615cdb8438 RBP: 0000000000000000 R08: 0000000002783333 R09: 0000000000000001 R10: ffff97605e6c4600 R11: 0000000000000001 R12: ffff97605e6c4c68 R13: 0000000000020000 R14: 0000000000000001 R15: ffff976064fe2c00 FS: 0000000000000000(0000) GS:ffff9776dfd400		

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
			00(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000008 CR3: 000000005942c002 CR4: 00000000001706f0 Call Trace: <TASK> ? __die+0x1f/0x70 ? page_fault_oops+0x15d/0x440 ? search_module_extables+0xe/0x40 ? fixup_exception+0x22/0x2f0 ? exc_page_fault+0x5f/0x100 ? asm_exc_page_fault+0x22/0x30 ? cachefiles_prepare_write+0x30/0xa0 netfs_rreq_write_to_cache_work+0x135/0x2e0		

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
			process_one_work +0x137/0x2c0 worker_thread+0x 2e9/0x400 ? __pfx_worker_threa d+0x10/0x10 kthread+0xcc/0x1 00 ? __pfx_kthread+0x1 0/0x10 ret_from_fork+0x3 0/0x50 ? __pfx_kthread+0x1 0/0x10 ret_from_fork_asm +0x1b/0x30 </TASK> Modules linked in: CR2: 000000000000000 8 ---[end trace 000000000000000 0]--- This happened because fscache_cookie_stat e_machine() was slow and was		

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
			still running while another process invoked fscache_unuse_cookie(); this led to a fscache_cookie_lru_do_one() call, setting the FSCACHE_COOKIE_DO_LRU_DISCARD flag, which was picked up by fscache_cookie_state_machine(), withdrawing the cookie via cachefiles_withdraw_cookie(), clearing cookie->cache_priv. At the same time, yet another process invoked cachefiles_prepare_write(), which found a NULL pointer in this code line: struct cachefiles_object *object = cachefiles_cres_object(cres); The next line crashes, obviously:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			struct cachefiles_cache *cache = object->volume->cache; During cachefiles_prepare_write(), the "n_accesses" counter is non-zero (via fscache_begin_operation()). The cookie must not be withdrawn until it drops to zero. The counter is checked by fscache_cookie_state_machine() before switching to FSCACHE_COOKIE_STATE_RELINQUISHING and FSCACHE_COOKIE_STATE_WITHDRAWING (in "case FSCACHE_COOKIE_STATE_FAILED"), but not for FSCACHE_COOKIE_STATE_LRU_DISCARDING ("case FSCACHE_COOKIE_STATE_ACTIVE").		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This patch adds the missing check. With a non-zero access counter, the function returns and the next fscache_end_cookie_access() call will queue another fscache_cookie_state_machine() call to handle the still-pending FSCACHE_COOKIE_DO_LRU_DISCARD. **CVE ID: CVE-2024-45000**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: rtla/osnoise: Prevent NULL dereference in error handling If the "tool->data" allocation fails then there is no need to call osnoise_free_top() and, in fact, doing so will lead to a NULL dereference. **CVE ID: CVE-2024-45002**	https://git.kernel.org/stable/c/753f1745146e03abd17eec8eee95faffc96d743d, https://git.kernel.org/stable/c/90574d2a675947858b47008df8d07f75ea50d0d0, https://git.kernel.org/stable/c/abdb9ddaaab476e62805e36cce7b4ef8413ffd01	O-LIN-LINU-190924/3223
NULL Pointer	04-Sep-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			vulnerability has been resolved: xhci: Fix Panther point NULL pointer deref at full-speed re-enumeration re-enumerating full-speed devices after a failed address device command can trigger a NULL pointer dereference. Full-speed devices may need to reconfigure the endpoint 0 Max Packet Size value during enumeration. Usb core calls usb_ep0_reinit() in this case, which ends up calling xhci_configure_end point(). On Panther point xHC the xhci_configure_end point() function will additionally check and reserve bandwidth in	0f0654318e25b 2c185e245ba4a 591e42fabb5e5 9, https://git.kern el.org/stable/c/ 365ef7c4277fd d781a695c355 3fa157d622d80 5d, https://git.kern el.org/stable/c/ 5ad898ae82412 f8a689d598298 04bff2999dd0e a	

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
			software. Other hosts do this in hardware If xHC address device command fails then a new xhci_virt_device structure is allocated as part of re-enabling the slot, but the bandwidth table pointers are not set up properly here. This triggers the NULL pointer dereference the next time usb_ep0_reinit() is called and xhci_configure_endpoint() tries to check and reserve bandwidth [46710.713538] usb 3-1: new full-speed USB device number 5 using xhci_hcd [46710.713699] usb 3-1: Device not responding to setup address. [46710.917684] usb 3-1: Device not responding to setup address.		

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
			[46711.125536] usb 3-1: device not accepting address 5, error -71 [46711.125594] BUG: kernel NULL pointer dereference, address: 0000000000000008 [46711.125600] #PF: supervisor read access in kernel mode [46711.125603] #PF: error_code(0x0000) - not-present page [46711.125606] PGD 0 P4D 0 [46711.125610] Oops: Oops: 0000 [#1] PREEMPT SMP PTI [46711.125615] CPU: 1 PID: 25760 Comm: kworker/1:2 Not tainted 6.10.3_2 #1 [46711.125620] Hardware name: Gigabyte Technology Co., Ltd. [46711.125623] Workqueue: usb_hub_wq hub_event [usbcore]		

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
			[46711.125668] RIP: 0010:xhci_reserve_bandwidth (drivers/usb/host/xhci.c Fix this by making sure bandwidth table pointers are set up correctly after a failed address device command, and additionally by avoiding checking for bandwidth in cases like this where no actual endpoints are added or removed, i.e. only context for default control endpoint 0 is evaluated. **CVE ID: CVE-2024-45006**		
N/A	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: only mark 'subflow' endp as available Adding the following warning ...	https://git.kernel.org/stable/c/322ea3778965da72862cca2a0c50253aacf65fe6, https://git.kernel.org/stable/c/43cf912b0b0fc7b4fd12cbc735d1f5afb8e1322d, https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3225

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
			WARN_ON_ONCE(msk->pm.local_addr_used == 0) ... before decrementing the local_addr_used counter helped to find a bug when running the "remove single address" subtest from the mptcp_join.sh selftests. Removing a 'signal' endpoint will trigger the removal of all subflows linked to this endpoint via mptcp_pm_nl_rm_addr_or_subflow() with rm_type == MPTCP_MIB_RMSUBFLOW. This will decrement the local_addr_used counter, which is wrong in this case because this counter is linked to 'subflow' endpoints, and here it is a 'signal'	7fdc870d08960961408a44c569f20f50940e7d4f	

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
			endpoint that is being removed. Now, the counter is decremented, only if the ID is being used outside of mptcp_pm_nl_rm_addr_or_subflow(), only for 'subflow' endpoints, and if the ID is not 0 -- local_addr_used is not taking into account these ones. This marking of the ID as being available, and the decrement is done no matter if a subflow using this ID is currently available, because the subflow could have been closed before. **CVE ID: CVE-2024-45010**		
N/A	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: char: xillybus: Check USB endpoints when probing device	https://git.kernel.org/stable/c/1371d32b95972d39c1e6e4bae8b6d0df1b573731, https://git.kernel.org/stable/c/2374bf7558de915edc6ec8cb10ec3291dfab959	O-LIN-LINU-190924/3226

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
			Ensure, as the driver probes the device, that all endpoints that the driver may attempt to access exist and are of the correct type. All XillyUSB devices must have a Bulk IN and Bulk OUT endpoint at address 1. This is verified in xillyusb_setup_base_eps(). On top of that, a XillyUSB device may have additional Bulk OUT endpoints. The information about these endpoints' addresses is deduced from a data structure (the IDT) that the driver fetches from the device while probing it. These endpoints are checked in setup_channels().	4, https://git.kernel.org/stable/c/25ee8b2908200fc862c0434e5ad483817d50ceda	

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
			A XillyUSB device never has more than one IN endpoint, as all data towards the host is multiplexed in this single Bulk IN endpoint. This is why setup_channels() only checks OUT endpoints. **CVE ID: CVE-2024-45011**		
Allocation of Resources Without Limits or Throttling	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nouveau/firmware: use dma non-coherent allocator Currently, enabling SG_DEBUG in the kernel will cause nouveau to hit a BUG() on startup, when the iommu is enabled: kernel BUG at include/linux/scatterlist.h:187! invalid opcode: 0000 [#1] PREEMPT SMP NOPTI CPU: 7 PID: 930 Comm: (udev-	https://git.kernel.org/stable/c/57ca481fca97ca4553e8c85d6a94baf4cb40c40e, https://git.kernel.org/stable/c/9b340aeb26d50e9a9ec99599e2a39b035fac978e, https://git.kernel.org/stable/c/cc29c5546c6a373648363ac49781f1d74b530707	O-LIN-LINU-190924/3227

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
			worker) Not tainted 6.9.0-rc3Lyude-Test+ #30 Hardware name: MSI MS-7A39/A320M GAMING PRO (MS-7A39), BIOS 1.I0 01/22/2019 RIP: 0010:sg_init_one+0x85/0xa0 Code: 69 88 32 01 83 e1 03 f6 c3 03 75 20 a8 01 75 1e 48 09 cb 41 89 54 24 08 49 89 1c 24 41 89 6c 24 0c 5b 5d 41 5c e9 7b b9 88 00 <0f> 0b 0f 0b 0f 0b 48 8b 05 5e 46 9a 01 eb b2 66 66 2e 0f 1f 84 00 RSP: 0018:ffffa776017bf6a0 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffffa77600d87000 RCX: 000000000000002b RDX: 0000000000000001 RSI: 0000000000000000 RDI: ffffa77680d87000		

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
			RBP: 000000000000e000 R08: 0000000000000000 R09: 0000000000000000 R10: ffff98f4c46aa508 R11: 0000000000000000 R12: ffff98f4c46aa508 R13: ffff98f4c46aa008 R14: ffffa77600d4a000 R15: ffffa77600d4a018 FS: 00007feeb5aae980(0000) GS:ffff98f5c4dc0000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f22cb9a4520 CR3: 00000001043ba000 CR4: 00000000003506f0 Call Trace: <TASK> ? die+0x36/0x90		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? do_trap+0xdd/0x100 ? sg_init_one+0x85/0xa0 ? do_error_trap+0x65/0x80 ? sg_init_one+0x85/0xa0 ? exc_invalid_op+0x50/0x70 ? sg_init_one+0x85/0xa0 ? asm_exc_invalid_op+0x1a/0x20 ? sg_init_one+0x85/0xa0 nvkm_firmware_ctor+0x14a/0x250 [nouveau] nvkm_falcon_fw_ctor+0x42/0x70 [nouveau] ga102_gsp_booter_ctor+0xb4/0x1a0 [nouveau] r535_gsp_oneinit+0xb3/0x15f0 [nouveau]		

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
			? srso_return_thunk+0x5/0x5f ? srso_return_thunk+0x5/0x5f ? nvkm_udevice_new+0x95/0x140 [nouveau] ? srso_return_thunk+0x5/0x5f ? srso_return_thunk+0x5/0x5f ? ktime_get+0x47/0xb0 Fix this by using the non-coherent allocator instead, I think there might be a better answer to this, but it involve ripping up some of APIs using sg lists. **CVE ID: CVE-2024-45012**		
Use After Free	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nvme: move stopping keep-alive	https://git.kernel.org/stable/c/4101af98ab573554c4225e328d506fec2a74bc54, https://git.kernel.org/stable/c/a54a93d0e3599	O-LIN-LINU-190924/3228

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
			into nvme_uninit_ctrl() Commit 4733b65d82bd ("nvme: start keep-alive after admin queue setup") moves starting keep-alive from nvme_start_ctrl() into nvme_init_ctrl_finish(), but don't move stopping keep-alive into nvme_uninit_ctrl(), so keep-alive work can be started and keep pending after failing to start controller, finally use-after-free is triggered if nvme host driver is unloaded. This patch fixes kernel panic when running nvme/004 in case that connection failure is triggered, by moving stopping keep-alive into nvme_uninit_ctrl(). This way is reasonable because	b05856971734e15418ac551a14c	

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
			keep-alive is now started in nvme_init_ctrl_finish(). **CVE ID: CVE-2024-45013**		
Allocation of Resources Without Limits or Throttling	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: s390/boot: Avoid possible physmem_info segment corruption When physical memory for the kernel image is allocated it does not consider extra memory required for offsetting the image start to match it with the lower 20 bits of KASLR virtual base address. That might lead to kernel access beyond its memory range. **CVE ID: CVE-2024-45014**	https://git.kernel.org/stable/c/a944cba5d57687b747023c3bc074fcf9c790f7df, https://git.kernel.org/stable/c/d7fd2941ae9a67423d1c7bee985f240e4686634f	O-LIN-LINU-190924/3229
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/3bacf814b6a61cc683c68465f1	O-LIN-LINU-190924/3230

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
			drm/msm/dpu: move dpu_encoder's connector assignment to atomic_enable() For cases where the crtc's connectors_changed was set without enable/active getting toggled , there is an atomic_enable() call followed by an atomic_disable() but without an atomic_mode_set(). This results in a NULL ptr access for the dpu_encoder_get_drm_fmt() call in the atomic_enable() as the dpu_encoder's connector was cleared in the atomic_disable() but not re-assigned as there was no atomic_mode_set() call. Fix the NULL ptr access by moving the assignment for	75ebd938f09c52, https://git.kernel.org/stable/c/3fb61718bcbe309279205d1cc275a6435611dc77, https://git.kernel.org/stable/c/aedf02e46eb549dac8db4821a6b9f0c6bf6e3990	

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
			atomic_enable() and also use drm_atomic_get_new_connector_for_encoder() to get the connector from the atomic_state. Patchwork: https://patchwork.freedesktop.org/patch/606729/ **CVE ID: CVE-2024-45015**		
Integer Overflow or Wraparound	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: workqueue: Fix UBSAN 'subtraction overflow' error in shift_and_mask() UBSAN reports the following 'subtraction overflow' error when booting in a virtual machine on Android: | Internal error: UBSAN: integer subtraction overflow: 00000000f200551	https://git.kernel.org/stable/c/38f7e14519d39cf524ddc02d4caee9b337dad703, https://git.kernel.org/stable/c/90a6a844b2d9927d192758438a4ada33d8cd9de5	O-LIN-LINU-190924/3231

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
			5 [#1] PREEMPT SMP | Modules linked in: | CPU: 0 PID: 1 Comm: swapper/0 Not tainted 6.10.0-00006-g3cbe9e5abd46-dirty #4 | Hardware name: linux,dummy-virt (DT) | pstate: 600000c5 (nZCv daIF -PAN -UAO -TCO -DIT -SSBS BTYPE=--) | pc : cancel_delayed_work+0x34/0x44 | lr : cancel_delayed_work+0x2c/0x44 | sp : ffff80008002ba60 | x29: ffff80008002ba60 x28: 0000000000000000 x27: 0000000000000000 | x26: 0000000000000000 x25: 0000000000000000 x24: 0000000000000000 | x23: 0000000000000000		

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 x22: 0000000000000000 x21: ffff1f65014cd3c0 | x20: ffffc0e84c9d0da0 x19: ffffc0e84cab3558 x18: ffff800080009058 | x17: 00000000247ee1f8 x16: 00000000247ee1f8 x15: 00000000bdcb279d | x14: 0000000000000001 x13: 0000000000000075 x12: 00000a0000000000 | x11: ffff1f6501499018 x10: 00984901651fffff x9 : ffff5e7cc35af000 | x8 : 0000000000000001 x7 : 3d4d455453595342 x6 : 000000004e514553 | x5 : ffff1f6501499265 x4 : ffff1f650ff60b10 x3 :		

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
			0000000000000620 | x2 : ffff80008002ba78 x1 : 0000000000000000 x0 : 0000000000000000 | Call trace: | cancel_delayed_work+0x34/0x44 | deferred_probe_extend_timeout+0x20/0x70 | driver_register+0xa8/0x110 | __platform_driver_register+0x28/0x3c | syscon_init+0x24/0x38 | do_one_initcall+0xe4/0x338 | do_initcall_level+0xac/0x178 | do_initcalls+0x5c/0xa0 | do_basic_setup+0x20/0x30		

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
			| kernel_init_freeable+0x8c/0xf8 | kernel_init+0x28/0x1b4 | ret_from_fork+0x10/0x20 | Code: f9000fbf 97fffa2f 39400268 37100048 (d42aa2a0) | ---[end trace 0000000000000000]--- | Kernel panic - not syncing: UBSAN: integer subtraction overflow: Fatal exception This is due to shift_and_mask() using a signed immediate to construct the mask and being called with a shift of 31 (WORK_OFFQ_POOL_SHIFT) so that it ends up decrementing from INT_MIN. Use an unsigned constant '1U' to generate the mask		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in shift_and_mask(). **CVE ID: CVE-2024-44981**		
N/A	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix IPsec RoCE MPV trace call Prevent the call trace below from happening, by not allowing IPsec creation over a slave, if master device doesn't support IPsec. WARNING: CPU: 44 PID: 16136 at kernel/locking/rwsem.c:240 down_read+0x75/0x94 Modules linked in: esp4_offload esp4 act_mirred act_vlan cls_flower sch_ingress mlx5_vdpa vringh vhost_iotlb vdpa mst_pciconf(OE) nfsv3 nfs_acl nfs lockd grace fscache netfs xt_CHECKSUM xt_MASQUERADE	https://git.kernel.org/stable/c/2ae52a65a850ded75a94e8d7ec1e09737f4c6509, https://git.kernel.org/stable/c/607e1df7bd47fe91cab85a97f57870a26d066137	O-LIN-LINU-190924/3232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			xt_conntrack ipt_REJECT nf_reject_ipv4 nft_compat nft_counter nft_chain_nat nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 rfkill cuse fuse rpcrdma sunrpc rdma_ucm ib_srpt ib_isert iscsi_target_mod target_core_mod ib_umad ib_iser libiscsi scsi_transport_iscsi rdma_cm ib_ipoib iw_cm ib_cm ipmi_ssif intel_rapl_msr intel_rapl_common amd64_edac edac_mce_amd kvm_amd kvm irqbypass crct10dif_pclmul crc32_pclmul mlx5_ib ghash_clmulni_intel sha1_ssse3 dell_smbios ib_uverbs aesni_intel crypto_simd dcdbas wmi_bmof dell_wmi_descriptor cryptd pcspkr ib_core acpi_ipmi sp5100_tco ccp i2c_piix4 ipmi_si ptdma k10temp ipmi_devintf		

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
			ipmi_msghandler acpi_power_meter acpi_cpufreq ext4 mbcache jbd2 sd_mod t10_pi sg mgag200 drm_kms_helper syscopyarea sysfillrect mlx5_core sysimgblt fb_sys_fops cec ahci libahci mlxfw drm pci_hyperv_intf libata tg3 sha256_ssse3 tls megaraid_sas i2c_algo_bit psample wmi dm_mirror dm_region_hash dm_log dm_mod [last unloaded: mst_pci] CPU: 44 PID: 16136 Comm: kworker/44:3 Kdump: loaded Tainted: GOE 5.15.0-20240509.el8uek.uek7_u3_update_v6.6_ipsec_bf.x86_64 #2 Hardware name: Dell Inc. PowerEdge R7525/074H08, BIOS 2.0.3 01/15/2021		

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
			Workqueue: events xfrm_state_gc_task RIP: 0010:down_read+0x75/0x94 Code: 00 48 8b 45 08 65 48 8b 14 25 80 fc 01 00 83 e0 02 48 09 d0 48 83 c8 01 48 89 45 08 5d 31 c0 89 c2 89 c6 89 c7 e9 cb 88 3b 00 <0f> 0b 48 8b 45 08 a8 01 74 b2 a8 02 75 ae 48 89 c2 48 83 ca 02 f0 RSP: 0018:ffffb26387773da8 EFLAGS: 00010282 RAX: 0000000000000000 RBX: ffffa08b658af900 RCX: 0000000000000001 RDX: 0000000000000000 RSI: ff886bc5e1366f2f RDI: 0000000000000000 RBP: ffffa08b658af940 R08: 0000000000000000 R09: 0000000000000000		

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
			R10: 0000000000000000 R11: 0000000000000000 R12: ffffa0a9bfb31540 R13: ffffa0a9bfb37900 R14: 0000000000000000 R15: ffffa0a9bfb37905 FS: 0000000000000000(0000) GS:ffffa0a9bfb00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000055a45ed814e8 CR3: 000000109038a000 CR4: 0000000000350ee0 Call Trace: <TASK> ? show_trace_log_lvl+0x1d6/0x2f9 ? show_trace_log_lvl+0x1d6/0x2f9 ? mlx5_devcom_for_each_peer_begin+0x		

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
			29/0x60 [mlx5_core] ? down_read+0x75/0x94 ? __warn+0x80/0x113 ? down_read+0x75/0x94 ? report_bug+0xa4/0x11d ? handle_bug+0x35/0x8b ? exc_invalid_op+0x14/0x75 ? asm_exc_invalid_op+0x16/0x1b ? down_read+0x75/0x94 ? down_read+0xe/0x94 mlx5_devcom_for_each_peer_begin+0x29/0x60 [mlx5_core] mlx5_ipsec_fs_roce_tx_destroy+0xb1/0x130 [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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tx_destroy+0x1b/0xc0 [mlx5_core] tx_ft_put+0x53/0xc0 [mlx5_core] mlx5e_xfrm_free_state+0x45/0x90 [mlx5_core] __xfrm_state_destroy+0x10f/0x1a2 xfrm_state_gc_task+0x81/0xa9 process_one_work+0x1f1/0x3c6 worker_thread+0x53/0x3e4 ? process_one_work.cold+0x46/0x3c kthread+0x127/0x144 ? set_kthread_struct+0x60/0x52 ret_from_fork+0x22/0x2d </TASK> ---[end trace 5ef7896144d398e1]---		

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
			CVE ID: CVE-2024-45017		
Improper Initialization	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: initialise extack before use Fix missing initialisation of extack in flow offload. **CVE ID: CVE-2024-45018**	https://git.kernel.org/stable/c/119be227bc04f5035efa64cb823b8a5ca5e2d1c1, https://git.kernel.org/stable/c/356beb911b63a8cff34cb57f755c2a2d2ee9dec7, https://git.kernel.org/stable/c/7eafeec6be68ebd6140a830ce9ae68ad5b67ec78	O-LIN-LINU-190924/3233
Improper Locking	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Take state lock during tx timeout reporter mlx5e_safe_reopen_channels() requires the state lock taken. The referenced changed in the Fixes tag removed the lock to fix another issue. This patch adds it back but at a later point (when calling	https://git.kernel.org/stable/c/03d3734bd692affe4d0e9c9d638f491aaf37411b, https://git.kernel.org/stable/c/8e57e66ecbdd2fddc9fbf3e984b1c523b70e9809, https://git.kernel.org/stable/c/b3b9a87adee97854bcd71057901d46943076267e	O-LIN-LINU-190924/3234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mlx5e_safe_reopen_channels()) to avoid the deadlock referenced in the Fixes tag. **CVE ID: CVE-2024-45019**		
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix a kernel verifier crash in stacksafe() Daniel Hodges reported a kernel verifier crash when playing with sched-ext. Further investigation shows that the crash is due to invalid memory access in stacksafe(). More specifically, it is the following code: if (exact != NOT_EXACT && old->stack[spi].slot_type[i % BPF_REG_SIZE] != cur->stack[spi].slot_typ	https://git.kernel.org/stable/c/6e3987ac310c74bb4dd6a2fa8e46702fe505fb2b, https://git.kernel.org/stable/c/7cad3174cc79519bf5f6c4441780264416822c08, https://git.kernel.org/stable/c/bed2eb964c70b780fb55925892a74f26cb590b25	O-LIN-LINU-190924/3235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			e[i % BPF_REG_SIZE]) return false; The 'i' iterates old->allocated_stack. If cur->allocated_stack < old->allocated_stack the out-of-bound access will happen. To fix the issue add 'i >= cur->allocated_stack' check such that if the condition is true, stacksafe() should fail. Otherwise, cur->stack[spi].slot_type[i % BPF_REG_SIZE] memory access is legal. **CVE ID: CVE-2024-45020**		
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: memcg_write_event_control(): fix a user-triggerable oops	https://git.kernel.org/stable/c/046667c4d3196938e992fba0dfcde570aa85cd0e, https://git.kernel.org/stable/c/0fbe2a72e853a1052abe9bc2b7df8ddb102da22	O-LIN-LINU-190924/3236

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
			we are *not* guaranteed that anything past the terminating NUL is mapped (let alone initialized with anything sane). **CVE ID: CVE-2024-45021**	7, https://git.kernel.org/stable/c/1b37ec85ad95b612307627758c6018cd9d92cca8	
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/vmalloc: fix page mapping if vm_area_alloc_pages() with high order fallback to order 0 The __vmap_pages_range_noflush() assumes its argument pages** contains pages with the same page shift. However, since commit e9c3cda4d86e ("mm, vmalloc: fix high order __GFP_NOFAIL allocations"), if gfp_flags includes __GFP_NOFAIL with high order in vm_area_alloc_page	https://git.kernel.org/stable/c/61ebe5a747da649057c37be1c37eb934b4af79ca, https://git.kernel.org/stable/c/c91618816f4d21fc574d7577a37722adcd4075b2, https://git.kernel.org/stable/c/de7bad86345c43cd040ed43e20d9fad78a3ee59f	O-LIN-LINU-190924/3237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			s() and page allocation failed for high order, the pages** may contain two different page shifts (high order and order-0). This could lead __vmap_pages_range_noflush() to perform incorrect mappings, potentially resulting in memory corruption. Users might encounter this as follows (vmap_allow_huge = true, 2M is for PMD_SIZE): kvmalloc(2M, __GFP_NOFAIL|GFP_X) __vmalloc_node_range_noprof(vm_flags=VM_ALLOW_HUGE_VMAP) vm_area_alloc_pages(order=9) ---> order-9 allocation failed and fallback to order-0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vmap_pages_range() vmap_pages_range_noflush() __vmap_pages_range_noflush(page_shift = 21) ----> wrong mapping happens We can remove the fallback code because if a high-order allocation fails, __vmalloc_node_range_noprof() will retry with order-0. Therefore, it is unnecessary to fallback to order-0 here. Therefore, fix this by removing the fallback code. **CVE ID: CVE-2024-45022**		
Use After Free	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netem: fix return value if duplicate enqueue fails	https://git.kernel.org/stable/c/0486d31dd8198e22b63a4730244b38fffce6d469, https://git.kernel.org/stable/c/52d99a69f3d556c6426048c9d481b912205919d8, https://git.kern	O-LIN-LINU-190924/3238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			There is a bug in netem_enqueue() introduced by commit 5845f706388a ("net: netem: fix skb length BUG_ON in __skb_to_sgvec") that can lead to a use-after-free. This commit made netem_enqueue() always return NET_XMIT_SUCCESS when a packet is duplicated, which can cause the parent qdisc's q.qlen to be mistakenly incremented. When this happens qlen_notify() may be skipped on the parent during destruction, leaving a dangling pointer for some classful qdiscs like DRR. There are two ways for the bug happen: - If the duplicated packet is dropped by rootq-	el.org/stable/c/577d6c0619467fe90f7e8e57e45cb5bd9d936014	

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
			>enqueue() and then the original packet is also dropped. - If rootq->enqueue() sends the duplicated packet to a different qdisc and the original packet is dropped. In both cases NET_XMIT_SUCCESS is returned even though no packets are enqueued at the netem qdisc. The fix is to defer the enqueue of the duplicate packet until after the original packet has been guaranteed to return NET_XMIT_SUCCESS. **CVE ID: CVE-2024-45016**		
Improper Locking	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: fix hugetlb vs. core-mm PT locking	https://git.kernel.org/stable/c/5f75cfbd6bb02295ddaed48adf667b6c828ce07b, https://git.kernel.org/stable/c/7300dadba49e5	O-LIN-LINU-190924/3239

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
			We recently made GUP's common page table walking code to also walk hugetlb VMAs without most hugetlb special-casing, preparing for the future of having less hugetlb-specific page table walking code in the codebase. Turns out that we missed one page table locking detail: page table locking for hugetlb folios that are not mapped using a single PMD/PUD. Assume we have hugetlb folio that spans multiple PTEs (e.g., 64 KiB hugetlb folios on arm64 with 4 KiB base page size). GUP, as it walks the page tables, will perform a pte_offset_map_lock() to grab the PTE table lock.	31af2d890ae4e34c9b115384a62	

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
			However, hugetlb that concurrently modifies these page tables would actually grab the mm->page_table_lock: with USE_SPLIT_PTE_PTLOCKS, the locks would differ. Something similar can happen right now with hugetlb folios that span multiple PMDs when USE_SPLIT_PMD_PTLOCKS. This issue can be reproduced [1], for example triggering: [3105.936100] ------------[cut here]------------ [3105.939323] WARNING: CPU: 31 PID: 2732 at mm/gup.c:142 try_grab_folio+0x11c/0x188 [3105.944634] Modules linked in: [...] [3105.974841] CPU: 31 PID: 2732 Comm: reproducer Not tainted 6.10.0-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			64.eln141.aarch64 #1 [3105.980406] Hardware name: QEMU KVM Virtual Machine, BIOS edk2-20240524-4.fc40 05/24/2024 [3105.986185] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [3105.991108] pc : try_grab_folio+0x11c/0x188 [3105.994013] lr : follow_page_pte+0xd8/0x430 [3105.996986] sp : ffff80008eafb8f0 [3105.999346] x29: ffff80008eafb900 x28: ffffffe8d481f380 x27: 00f80001207cff43 [3106.004414] x26: 0000000000000001 x25: 0000000000000000 x24: ffff80008eafba48 [3106.009520] x23: 0000ffff9372f000 x22: ffff7a54459e2000		

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
			x21: ffff7a546c1aa978 [3106.014529] x20: ffffffe8d481f3c0 x19: 0000000000610041 x18: 0000000000000001 [3106.019506] x17: 0000000000000001 x16: ffffffffffffffff x15: 0000000000000000 [3106.024494] x14: ffffb85477fdfe08 x13: 0000ffff9372ffff x12: 0000000000000000 [3106.029469] x11: 1fffef4a88a96be1 x10: ffff7a54454b5f0c x9 : ffffb854771b12f0 [3106.034324] x8 : 0008000000000000 x7 : ffff7a546c1aa980 x6 : 0008000000000080 [3106.038902] x5 : 00000000001207cf x4 :		

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
			0000ffff9372f000 x3 : ffffffe8d481f000 [3106.043420] x2 : 0000000000610041 x1 : 0000000000000001 x0 : 0000000000000000 [3106.047957] Call trace: [3106.049522] try_grab_folio+0x11c/0x188 [3106.051996] follow_pmd_mask.constprop.0.isra.0+0x150/0x2e0 [3106.055527] follow_page_mask+0x1a0/0x2b8 [3106.058118] __get_user_pages+0xf0/0x348 [3106.060647] faultin_page_range+0xb0/0x360 [3106.063651] do_madvise+0x340/0x598 Let's make huge_pte_lockptr() effectively use the same PT locks as any core-mm page table walker would. Add		

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
			ptep_lockptr() to obtain the PTE page table lock using a pte pointer -- unfortunately we cannot convert pte_lockptr() because virt_to_page() doesn't work with kmap'ed page tables we can have with CONFIG_HIGHPTE. Handle CONFIG_PGTABLE_LEVELS correctly by checking in reverse order, such that when e.g., CONFIG_PGTABLE_LEVELS==2 with PGDIR_SIZE==P4D_SIZE==PUD_SIZE==PMD_SIZE will work as expected. Document why that works. There is one ugly case: powerpc 8xx, whereby we have an 8 MiB hugetlb folio being mapped using two PTE page tables. While hugetlb wants to take		

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 PMD table lock, core-mm would grab the PTE table lock of one of both PTE page tables. In such corner cases, we have to make sure that both locks match, which is (fortunately!) currently guaranteed for 8xx as it does not support SMP and consequently doesn't use split PT locks. [1] https://lore.kernel.org/all/1bbfcc7f-f222-45a5-ac44-c5a1381c596d@redhat.com/ **CVE ID: CVE-2024-45024**		
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fix bitmap corruption on close_range() with CLOSE_RANGE_UNSHARE copy_fd_bitmaps(new, old, count) is	https://git.kernel.org/stable/c/5053581fe5dfb09b58c65dd8462bf5dea71f41ff, https://git.kernel.org/stable/c/8cad3b2b3ab81ca55f37405ffd1315bcc2948058, https://git.kernel.org/stable/c/9a2fa14720835	O-LIN-LINU-190924/3240

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
			expected to copy the first count/BITS_PER_LONG bits from old->full_fds_bits[] and fill the rest with zeroes. What it does is copying enough words (BITS_TO_LONGS(count/BITS_PER_LONG)), then memsets the rest. That works fine, *if* all bits past the cutoff point are clear. Otherwise we are risking garbage from the last word we'd copied. For most of the callers that is true - expand_fdtable() has count equal to old->max_fds, so there's no open descriptors past count, let alone fully occupied words in ->open_fds[], which is what bits in ->full_fds_bits[] correspond to.	80b6c66bdaf291f591e1170123a	

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 other caller (dup_fd()) passes sane_fdtable_size(old_fdt, max_fds), which is the smallest multiple of BITS_PER_LONG that covers all opened descriptors below max_fds. In the common case (copying on fork()) max_fds is ~0U, so all opened descriptors will be below it and we are fine, by the same reasons why the call in expand_fdtable() is safe. Unfortunately, there is a case where max_fds is less than that and where we might, indeed, end up with junk in ->full_fds_bits[] - close_range(from, to, CLOSE_RANGE_UNSHARE) with * descriptor table being currently shared * 'to' being above the current		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			capacity of descriptor table * 'from' being just under some chunk of opened descriptors. In that case we end up with observably wrong behaviour - e.g. spawn a child with CLONE_FILES, get all descriptors in range 0..127 open, then close_range(64, ~0U, CLOSE_RANGE_UNSHARE) and watch dup(0) ending up with descriptor #128, despite #64 being observably not open. The minimally invasive fix would be to deal with that in dup_fd(). If this proves to add measurable overhead, we can go that way, but let's try to fix copy_fd_bitmaps() first. * new helper: bitmap_copy_and_e		

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
			xpand(to, from, bits_to_copy, size). * make copy_fd_bitmaps() take the bitmap size in words, rather than bits; it's 'count' argument is always a multiple of BITS_PER_LONG, so we are not losing any information, and that way we can use the same helper for all three bitmaps - compiler will see that count is a multiple of BITS_PER_LONG for the large ones, so it'll generate plain memcpy()+memset(). Reproducer added to tools/testing/selftests/core/close_range_test.c **CVE ID: CVE-2024-45025**		
Improper Initialization	02-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/18a067240817bee8a9360539af5d79a4bf5398a5, https://git.kern	O-LIN-LINU-190924/3241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fuse: Initialize beyond-EOF page contents before setting uptodate fuse_notify_store(), unlike fuse_do_readpage(), does not enable page zeroing (because it can be used to change partial page contents). So fuse_notify_store() must be more careful to fully initialize page contents (including parts of the page that are beyond end-of-file) before marking the page uptodate. The current code can leave beyond-EOF page contents uninitialized, which makes these uninitialized page contents visible to userspace via mmap(). This is an information leak, but only affects	el.org/stable/c/33168db352c7b56ae18aa55c2cae1a1c5905d30e, https://git.kernel.org/stable/c/3c0da3d163eb32f1f91891efaade027fa9b245b9	

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
			systems which do not enable init-on-alloc (via CONFIG_INIT_ON_ALLOC_DEFAULT_ON=y or the corresponding kernel command line parameter). **CVE ID: CVE-2024-44947**		
Incomplete Cleanup	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: xhci: Check for xhci->interrupters being allocated in xhci_mem_clearup() If xhci_mem_init() fails, it calls into xhci_mem_cleanup() to mop up the damage. If it fails early enough, before xhci->interrupters is allocated but after xhci->max_interrupters has been set, which happens in most (all?) cases, things get uglier, as xhci_mem_cleanup()	https://git.kernel.org/stable/c/770cacc75b0091ece17349195d72133912c1ca7c, https://git.kernel.org/stable/c/dcdb52d948f3a17ccd3fce757d9bd981d7c32039	O-LIN-LINU-190924/3242

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
			unconditionally derefences xhci->interrupters. With prejudice. Gate the interrupt freeing loop with a check on xhci->interrupters being non-NULL. Found while debugging a DMA allocation issue that led the XHCI driver on this exact path. **CVE ID: CVE-2024-45027**		
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mmc: mmc_test: Fix NULL dereference on allocation failure If the "test->highmem = alloc_pages()" allocation fails then calling __free_pages(test->highmem) will result in a NULL dereference. Also	https://git.kernel.org/stable/c/2b507b03991f44dfb202fc2a82c9874d1b1f0c06, https://git.kernel.org/stable/c/3b4e76ceae5b5a46c968bd952f551ce173809f63, https://git.kernel.org/stable/c/9b9ba386d7bfdbc38445932c90fa9444c0524bea	O-LIN-LINU-190924/3243

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
			change the error code to -ENOMEM instead of returning success. **CVE ID: CVE-2024-45028**		
Improper Locking	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: i2c: tegra: Do not mark ACPI devices as irq safe On ACPI machines, the tegra i2c module encounters an issue due to a mutex being called inside a spinlock. This leads to the following bug: BUG: sleeping function called from invalid context at kernel/locking/mutex.c:585 ... Call trace: __might_sleep __mutex_lock_common mutex_lock_nested	https://git.kernel.org/stable/c/14d069d92951a3e150c0a81f2ca3b93e54da913b, https://git.kernel.org/stable/c/2853e1376d8161b04c9ff18ba82b43f08a049905, https://git.kernel.org/stable/c/6861faf4232e4b78878f2de1ed3ee324ddae2287	O-LIN-LINU-190924/3244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			acpi_subsys_runtime_resume rpm_resume tegra_i2c_xfer The problem arises because during __pm_runtime_resume(), the spinlock &dev->power.lock is acquired before rpm_resume() is called. Later, rpm_resume() invokes acpi_subsys_runtime_resume(), which relies on mutexes, triggering the error. To address this issue, devices on ACPI are now marked as not IRQ-safe, considering the dependency of acpi_subsys_runtime_resume() on mutexes. **CVE ID: CVE-2024-45029**		
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/8aba27c4a5020abdf60149239198297f88338a8d,	O-LIN-LINU-190924/3245

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
			igb: cope with large MAX_SKB_FRAGS Sabrina reports that the igb driver does not cope well with large MAX_SKB_FRAG values: setting MAX_SKB_FRAG to 45 causes payload corruption on TX. An easy reproducer is to run ssh to connect to the machine. With MAX_SKB_FRAGS= 17 it works, with MAX_SKB_FRAGS= 45 it fails. This has been reported originally in https://bugzilla.redhat.com/show_bug.cgi?id=2265320 The root cause of the issue is that the driver does not take into account properly the (possibly large) shared info size when selecting the ring layout, and will try to fit two packets inside the same 4K	https://git.kernel.org/stable/c/8ea80ff5d8298356d28077bc30913ed37df65109, https://git.kernel.org/stable/c/b52bd8bcb9e8ff250c79b44f9af8b15cae8911ab	

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
			page even when the 1st fraglist will trump over the 2nd head. Address the issue by checking if 2K buffers are insufficient. **CVE ID: CVE-2024-45030**		
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: cfg80211: Handle SSID based pmksa deletion wpa_supplicant 2.11 sends since 1efdba5fdc2c ("Handle PMKSA flush in the driver for SAE/OWE offload cases") SSID based PMKSA del commands. brcmfmac is not prepared and tries to dereference the NULL bssid and pmkid pointers in cfg80211_pmksa. PMKID_V3 operations support SSID based	https://git.kernel.org/stable/c/1f566eb912d192c83475a919331aea59619e1197, https://git.kernel.org/stable/c/2ad4e1ada8eebafa2d75a4b75eeeca882de6ada1, https://git.kernel.org/stable/c/4291f94f8c6b01505132c22ee27b59ed27c3584f	O-LIN-LINU-190924/3246

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
			updates so copy the SSID. **CVE ID: CVE-2024-46672**		
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: driver core: Fix uevent_show() vs driver detach race uevent_show() wants to de-reference dev->driver->name. There is no clean way for a device attribute to de-reference dev->driver unless that attribute is defined via (struct device_driver).dev_groups. Instead, the anti-pattern of taking the device_lock() in the attribute handler risks deadlocks with code paths that remove device attributes while holding the lock. This deadlock is typically invisible	https://git.kernel.org/stable/c/15fffc6a5624b13b428bb1c6e9088e32a55eb82c, https://git.kernel.org/stable/c/49ea4e0d862632d51667da5e7a9c88a560e9c5a1, https://git.kernel.org/stable/c/4a7c2a8387524942171037e70b80e969c3b5c05b	O-LIN-LINU-190924/3247

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
			to lockdep given the device_lock() is marked lockdep_set_novalidate_class(), but some subsystems allocate a local lockdep key for @dev->mutex to reveal reports of the form: ========== ========== ========== ========= WARNING: possible circular locking dependency detected 6.10.0-rc7+ #275 Tainted: G OE N ---------- ---------- modprobe/2374 is trying to acquire lock: ffff8c2270070de0 (kn->active#6){++++}-{0:0}, at: __kernfs_remove+0xde/0x220 but task is already holding lock:		

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
			ffff8c22016e88f8 (&cxl_root_key){+.+.}-{3:3}, at: device_release_driver_internal+0x39/0x210 which lock already depends on the new lock. the existing dependency chain (in reverse order) is: -> #1 (&cxl_root_key){+.+.}-{3:3}: __mutex_lock+0x99/0xc30 uevent_show+0xac/0x130 dev_attr_show+0x18/0x40 sysfs_kf_seq_show+0xac/0xf0 seq_read_iter+0x110/0x450 vfs_read+0x25b/0x340		

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
			ksys_read+0x67/0xf0 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e -> #0 (kn->active#6){++++}-{0:0}: __lock_acquire+0x121a/0x1fa0 lock_acquire+0xd6/0x2e0 kernfs_drain+0x1e9/0x200 __kernfs_remove+0xde/0x220 kernfs_remove_by_name_ns+0x5e/0xa0 device_del+0x168/0x410 device_unregister+0x13/0x60 devres_release_all+0xb8/0x110		

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
			device_unbind_cleanup+0xe/0x70 device_release_driver_internal+0x1c7/0x210 driver_detach+0x47/0x90 bus_remove_driver+0x6c/0xf0 cxl_acpi_exit+0xc/0x11 [cxl_acpi] __do_sys_delete_module.isra.0+0x181/0x260 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e The observation though is that driver objects are typically much longer lived than device objects. It is reasonable to perform lockless de-reference of a @driver pointer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			even if it is racing detach from a device. Given the infrequency of driver unregistration, use synchronize_rcu() in module_remove_driver() to close any potential races. It is potentially overkill to suffer synchronize_rcu() just to handle the rare module removal racing uevent_show() event. Thanks to Tetsuo Handa for the debug analysis of the syzbot report [1]. **CVE ID: CVE-2024-44952**		
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Fix deadlock during RTC update There is a deadlock when runtime	https://git.kernel.org/stable/c/3911af778f208e5f49d43ce739332b91e26bc48e, https://git.kernel.org/stable/c/f13f1858a28c68b7fc0d72c2008d5c1f80d2e8d5	O-LIN-LINU-190924/3248

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
			suspend waits for the flush of RTC work, and the RTC work calls ufshcd_rpm_get_sync() to wait for runtime resume. Here is deadlock backtrace: kworker/0:1 D 4892.876354 10 10971 4859 0x4208060 0x8 10 0 120 670730152367 ptr f0ffff80c2e40000 01 0x00000001 0x000000ff 0x000000ff 0x000000ff <ffffffee5e71ddb0>__switch_to+0x1a8/0x2d4 <ffffffee5e71e604>__schedule+0x684/0xa98 <ffffffee5e71ea60>schedule+0x48/0xc8 <ffffffee5e725f78>schedule_timeout+0x48/0x170 <ffffffee5e71fb74>do_wait_for_common+0x108/0x1b0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<ffffffee5e71efe0> wait_for_completion+0x44/0x60 <ffffffee5d6de968> __flush_work+0x39c/0x424 <ffffffee5d6decc0> __cancel_work_sync+0xd8/0x208 <ffffffee5d6dee2c> cancel_delayed_work_sync+0x14/0x28 <ffffffee5e2551b8> __ufshcd_wl_suspend+0x19c/0x480 <ffffffee5e255fb8> ufshcd_wl_runtime_suspend+0x3c/0x1d4 <ffffffee5dffd80c> scsi_runtime_suspend+0x78/0xc8 <ffffffee5df93580> __rpm_callback+0x94/0x3e0 <ffffffee5df90b0c> rpm_suspend+0x2d4/0x65c <ffffffee5df91448> __pm_runtime_suspend+0x80/0x114 <ffffffee5dffd95c> scsi_runtime_idle+0x38/0x6c <ffffffee5df912f4> rpm_idle+0x264/0x338		

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
			<ffffffee5df90f14> __pm_runtime_idle +0x80/0x110 <ffffffee5e24ce44> ufshcd_rtc_work+0 x128/0x1e4 <ffffffee5d6e3a40> process_one_work +0x26c/0x650 <ffffffee5d6e65c8> worker_thread+0x 260/0x3d8 <ffffffee5d6edec8> kthread+0x110/0x 134 <ffffffee5d616b18> ret_from_fork+0x1 0/0x20 Skip updating RTC if RPM state is not RPM_ACTIVE. **CVE ID: CVE-2024-44953**		
NULL Pointer Dereferenc e	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: gtp: fix a potential NULL pointer dereference When sockfd_lookup() fails, gtp_encap_enable_s ocket() returns a	https://git.kern el.org/stable/c/ 28c67f0f84f889 fe9f4cbda83541 32b20dc9212d, https://git.kern el.org/stable/c/ 4643b91691e9 69b1b9ad54bf5 52d7a990cfa3b 87, https://git.kern el.org/stable/c/ 612edd35f2a39 10ab1f61c1f23 38889d4ba99fa 2	O-LIN-LINU-190924/3249

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
			NULL pointer, but its callers only check for error pointers thus miss the NULL pointer case. Fix it by returning an error pointer with the error code carried from sockfd_lookup(). (I found this bug during code inspection.) **CVE ID: CVE-2024-46677**		
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nfsd: prevent panic for nfsv4.0 closed files in nfs4_show_open Prior to commit 3f29cc82a84c ("nfsd: split sc_status out of sc_type") states_show() relied on sc_type field to be of valid type before calling into a subfunction to show content of a	https://git.kernel.org/stable/c/a204501e1743d695ca2930ed25a2be9f8ced96d3, https://git.kernel.org/stable/c/ba0b697de298285301c71c258598226e06494236	O-LIN-LINU-190924/3250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			particular stateid. From that commit, we split the validity of the stateid into sc_status and no longer changed sc_type to 0 while unhashing the stateid. This resulted in kernel oopsing for nfsv4.0 opens that stay around and in nfs4_show_open() would derefence sc_file which was NULL. Instead, for closed open stateids forgo displaying information that relies of having a valid sc_file. To reproduce: mount the server with 4.0, read and close a file and then on the server cat /proc/fs/nfsd/clients/2/states [513.590804] Call trace:		

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
			[513.590925] _raw_spin_lock+0xcc/0x160 [513.591119] nfs4_show_open+0x78/0x2c0 [nfsd] [513.591412] states_show+0x44c/0x488 [nfsd] [513.591681] seq_read_iter+0x5d8/0x760 [513.591896] seq_read+0x188/0x208 [513.592075] vfs_read+0x148/0x470 [513.592241] ksys_read+0xcc/0x178 **CVE ID: CVE-2024-46682**		
Missing Release of Memory after Effective Lifetime	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: dsa: bcm_sf2: Fix a possible memory leak in bcm_sf2_mdio_register() bcm_sf2_mdio_register() calls of_phy_find_device() and then phy_device_remove() in a loop to	https://git.kernel.org/stable/c/7feef10768ea71d468d9bbc1e0d14c461876768c, https://git.kernel.org/stable/c/a7d2808d67570e6acae45c2a96e0d59986888e4c, https://git.kernel.org/stable/c/b7b8d9f5e679af60c94251fd6728dde34be69a71	O-LIN-LINU-190924/3251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remove existing PHY devices. of_phy_find_device() eventually calls bus_find_device(), which calls get_device() on the returned struct device * to increment the refcount. The current implementation does not decrement the refcount, which causes memory leak. This commit adds the missing phy_device_free() call to decrement the refcount via put_device() to balance the refcount. **CVE ID: CVE-2024-44971**		
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: pinctrl: single: fix potential NULL dereference in pcs_get_function()	https://git.kernel.org/stable/c/0a2bab5ed161318f57134716acba0a30f3af191, https://git.kernel.org/stable/c/1c38a62f15e595346a1106025722869e87ffe044,	O-LIN-LINU-190924/3252

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
			pinmux_generic_get_function() can return NULL and the pointer 'function' was dereferenced without checking against NULL. Add checking of pointer 'function' in pcs_get_function(). Found by code review. **CVE ID: CVE-2024-46685**	https://git.kernel.org/stable/c/292151af6add3e5ab11b2e9916cffa5f52859a1f	
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: smb/client: avoid dereferencing rdata=NULL in smb2_new_read_req() This happens when called from SMB2_read() while using rdma and reaching the rdma_readwrite_threshold. **CVE ID: CVE-2024-46686**	https://git.kernel.org/stable/c/6df57c63c200cd05e085c3b695128260e21959b7, https://git.kernel.org/stable/c/a01859dd6aebf826576513850a3b05992809e9d2, https://git.kernel.org/stable/c/b902fb78ab21299e4dd1775e7e8d251d5c0735bc	O-LIN-LINU-190924/3253
N/A	11-Sep-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/1c1f721375989579e46741f595	O-LIN-LINU-190924/3254

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
			vulnerability has been resolved: mptcp: pm: only decrement add_addr_accepted for MPJ req Adding the following warning ... WARN_ON_ONCE(msk->pm.add_addr_accepted == 0) ... before decrementing the add_addr_accepted counter helped to find a bug when running the "remove single subflow" subtest from the mptcp_join.sh selftest. Removing a 'subflow' endpoint will first trigger a RM_ADDR, then the subflow closure. Before this patch, and upon the reception of the	23e39ec9b2a9bd, https://git.kernel.org/stable/c/2060f1efab370b496c4903b840844ecaff324c3c, https://git.kernel.org/stable/c/35b31f5549ede4070566b949781e83495906b43d	

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
			RM_ADDR, the other peer will then try to decrement this add_addr_accepted. That's not correct because the attached subflows have not been created upon the reception of an ADD_ADDR. A way to solve that is to decrement the counter only if the attached subflow was an MP_JOIN to a remote id that was not 0, and initiated by the host receiving the RM_ADDR. **CVE ID: CVE-2024-45009**		
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: typec: ucsi: Move unregister out of atomic section Commit '9329933699b3 ("soc: qcom:	https://git.kernel.org/stable/c/095b0001aefddcd9361097c971b7debc84e72714, https://git.kernel.org/stable/c/11bb2ffb679399f99041540cf662409905179e3a	O-LIN-LINU-190924/3255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pmic_glink: Make client-lock non-sleeping")' moved the pmic_glink client list under a spinlock, as it is accessed by the rpmsg/glink callback, which in turn is invoked from IRQ context. This means that ucsi_unregister() is now called from atomic context, which isn't feasible as it's expecting a sleepable context. An effort is under way to get GLINK to invoke its callbacks in a sleepable context, but until then lets schedule the unregistration. A side effect of this is that ucsi_unregister() can now happen after the remote processor, and thereby the communication link with it, is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gone. pmic_glink_send() is amended with a check to avoid the resulting NULL pointer dereference. This does however result in the user being informed about this error by the following entry in the kernel log: ucsi_glink.pmic_glink_ucsi pmic_glink.ucsi.0: failed to send UCSI write request: -5 **CVE ID: CVE-2024-46691**		
Improper Locking	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: firmware: qcom: scm: Mark get_wq_ctx() as atomic call Currently get_wq_ctx() is wrongly configured as a standard call. When two SMC calls are in sleep and one SMC	https://git.kernel.org/stable/c/9960085a3a82c58d3323c1c20b991db6045063b0, https://git.kernel.org/stable/c/cdf7efe4b02aa93813db0bf1ca596ad298ab6b06, https://git.kernel.org/stable/c/e40115c33c0d79c940545b6b12112aace7acd9f5	O-LIN-LINU-190924/3256

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
			wakes up, it calls get_wq_ctx() to resume the corresponding sleeping thread. But if get_wq_ctx() is interrupted, goes to sleep and another SMC call is waiting to be allocated a waitq context, it leads to a deadlock. To avoid this get_wq_ctx() must be an atomic call and can't be a standard SMC call. Hence mark get_wq_ctx() as a fast call. **CVE ID: CVE-2024-46692**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bonding: fix xfrm real_dev null pointer dereference We shouldn't set real_dev to NULL because packets can be in transit and	https://git.kernel.org/stable/c/21816b696c172c19d53a30d45ee005cce246ed21, https://git.kernel.org/stable/c/2f72c6a66bcd7e0187ec085237fee5db27145294, https://git.kernel.org/stable/c/4582d4ff413a07d4ed8a4823c6	O-LIN-LINU-190924/3257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			xfrm might call xdo_dev_offload_ok() in parallel. All callbacks assume real_dev is set. Example trace: kernel: BUG: unable to handle page fault for address: 0000000000001030 kernel: bond0: (slave eni0np1): making interface the new active one kernel: #PF: supervisor write access in kernel mode kernel: #PF: error_code(0x0002) - not-present page kernel: PGD 0 P4D 0 kernel: Oops: 0002 [#1] PREEMPT SMP kernel: CPU: 4 PID: 2237 Comm: ping Not tainted 6.7.7+ #12 kernel: Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014	52dc5207760548	

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
			kernel: RIP: 0010:nsim_ipsec_offload_ok+0xc/0x20 [netdevsim] kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: Code: e0 0f 0b 48 83 7f 38 00 74 de 0f 0b 48 8b 47 08 48 8b 37 48 8b 78 40 e9 b2 e5 9a d7 66 90 0f 1f 44 00 00 48 8b 86 80 02 00 00 <83> 80 30 10 00 00 01 b8 01 00 00 00 c3 0f 1f 80 00 00 00 00 0f 1f kernel: bond0: (slave eni0np1): making interface the new active one kernel: RSP: 0018:ffffabde81553b98 EFLAGS: 00010246 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: kernel: RAX: 0000000000000000 RBX: ffff9eb404e74900 RCX: ffff9eb403d97c60 kernel: RDX: ffffffffc090de10 RSI:		

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
			ffff9eb404e74900 RDI: ffff9eb3c5de9e00 kernel: RBP: ffff9eb3c0a42000 R08: 0000000000000010 R09: 0000000000000014 kernel: R10: 7974203030303030 R11: 3030303030303030 R12: 0000000000000000 kernel: R13: ffff9eb3c5de9e00 R14: ffffabde81553cc8 R15: ffff9eb404c53000 kernel: FS: 00007f2a77a3ad00(0000) GS:ffff9eb43bd00000(0000) knlGS:0000000000000000 kernel: CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 kernel: CR2: 0000000000001030 CR3: 00000001122ab000 CR4: 0000000000350ef0		

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
			kernel: bond0: (slave eni0np1): making interface the new active one kernel: Call Trace: kernel: <TASK> kernel: ? __die+0x1f/0x60 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ? page_fault_oops+0x142/0x4c0 kernel: ? do_user_addr_fault+0x65/0x670 kernel: ? kvm_read_and_reset_apf_flags+0x3b/0x50 kernel: bond0: (slave eni0np1): making interface the new active one kernel: ? exc_page_fault+0x7b/0x180 kernel: ? asm_exc_page_fault+0x22/0x30 kernel: ? nsim_bpf_uninit+0x50/0x50 [netdevsim] kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA		

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
			kernel: ? nsim_ipsec_offload_ok+0xc/0x20 [netdevsim] kernel: bond0: (slave eni0np1): making interface the new active one kernel: bond_ipsec_offload_ok+0x7b/0x90 [bonding] kernel: xfrm_output+0x61/0x3b0 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ip_push_pending_frames+0x56/0x80 **CVE ID: CVE-2024-44989**		
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: video/aperture: optionally match the device in sysfb_disable() In aperture_remove_conflicting_pci_devices(), we currently only	https://git.kernel.org/stable/c/17e78f43de0c6da34204cc858b4cc05671ea9acf, https://git.kernel.org/stable/c/b49420d6a1aeb399e5b107fc6eb8584d0860fbd7	O-LIN-LINU-190924/3258

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
			call sysfb_disable() on vga class devices. This leads to the following problem when the pimary device is not VGA compatible: 1. A PCI device with a non-VGA class is the boot display 2. That device is probed first and it is not a VGA device so sysfb_disable() is not called, but the device resources are freed by aperture_detach_platform_device() 3. Non-primary GPU has a VGA class and it ends up calling sysfb_disable() 4. NULL pointer dereference via sysfb_disable() since the resources have already been freed by aperture_detach_platform_device() when it was called by the other device.		

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
			Fix this by passing a device pointer to sysfb_disable() and checking the device to determine if we should execute it or not. v2: Fix build when CONFIG_SCREEN_INFO is not set v3: Move device check into the mutex Drop primary variable in aperture_remove_conflicting_pci_devices() Drop __init on pci sysfb_pci_dev_is_enabled() **CVE ID: CVE-2024-46698**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bonding: fix null pointer deref in bond_ipsec_offload_ok We must check if there is an active slave before dereferencing the pointer.	https://git.kernel.org/stable/c/0707260a18312bbcd2a5668584e3692d0a29e3f6, https://git.kernel.org/stable/c/2f5bdd68c1ce64bda6bef4d361a3de23b04ccd59, https://git.kernel.org/stable/c/32a0173600c63aadaf2103bf0	O-LIN-LINU-190924/3259

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
			CVE ID: CVE-2024-44990	2f074982e8602ab	
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: smb/client: avoid possible NULL dereference in cifs_free_subrequest() Clang static checker (scan-build) warning: cifsglob.h:line 890, column 3 Access to field 'ops' results in a dereference of a null pointer. Commit 519be989717c ("cifs: Add a tracepoint to track credits involved in R/W requests") adds a check for 'rdata->server', and let clang throw this warning about NULL dereference. When 'rdata->credits.value != 0 && rdata->server == NULL' happens,	https://git.kernel.org/stable/c/74c2ab6d653b4c2354df65a7f7f2df1925a40a51, https://git.kernel.org/stable/c/fead60a6d5f84b472b928502a42c419253afe6c1	O-LIN-LINU-190924/3260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			add_credits_and_wake_if() will call rdata->server->ops->add_credits(). This will cause NULL dereference problem. Add a check for 'rdata->server' to avoid NULL dereference. **CVE ID: CVE-2024-44992**		
NULL Pointer Dereference	13-Sep-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: soc: qcom: pmic_glink: Fix race during initialization As pointed out by Stephen Boyd it is possible that during initialization of the pmic_glink child drivers, the protection-domain notifiers fires, and the associated work is scheduled, before the client registration returns and as a result the local	https://git.kernel.org/stable/c/1efdbf5323c9360e05066049b97414405e94e087, https://git.kernel.org/stable/c/3568affcddd68743e25aa3ec1647d9b82797757b, https://git.kernel.org/stable/c/943b0e7cc646a624bb20a68080f8f1a4a55df41c	O-LIN-LINU-190924/3261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"client" pointer has been initialized. The outcome of this is a NULL pointer dereference as the "client" pointer is blindly dereferenced. Timeline provided by Stephen: CPU0 CPU1 ---- --- ucsi->client = NULL; devm_pmic_glink_register_client() client->pdr_notify(client->priv, pg->client_state) pmic_glink_ucsi_pdr_notify() schedule_work(&ucsi->register_work) <schedule away> pmic_glink_ucsi_register() ucsi_register()		

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
			pmic_glink_ucsi_read_version() pmic_glink_ucsi_read() pmic_glink_ucsi_read() pmic_glink_send(ucsi->client) <client is NULL BAD> ucsi->client = client // Too late! This code is identical across the altmode, battery manager and usci child drivers. Resolve this by splitting the allocation of the "client" object and the registration thereof into two operations. This only happens if the protection domain registry is populated at the time of registration, which by the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			introduction of commit '1ebcde047c54 ("soc: qcom: add pd-mapper implementation")' became much more likely. **CVE ID: CVE-2024-46693**		
Affected Version(s): 6.2.3					
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: smb/client: avoid dereferencing rdata=NULL in smb2_new_read_req() This happens when called from SMB2_read() while using rdma and reaching the rdma_readwrite_threshold. **CVE ID: CVE-2024-46686**	https://git.kernel.org/stable/c/6df57c63c200cd05e085c3b695128260e21959b7, https://git.kernel.org/stable/c/a01859dd6aebf826576513850a3b05992809e9d2, https://git.kernel.org/stable/c/b902fb78ab21299e4dd1775e7e8d251d5c0735bc	O-LIN-LINU-190924/3262
Affected Version(s): From (including) 2.6.12 Up to (excluding) 4.19.321					
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: atm: idt77252: prevent use after	https://git.kernel.org/stable/c/09e086a5f72ea27c758b3f3b419a69000c32adc1, https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			free in dequeue_rx() We can't dereference "skb" after calling vcc->push() because the skb is released. **CVE ID: CVE-2024-44998**	1cece837e387c039225f19028df255df87a97c0d, https://git.kernel.org/stable/c/24cf390a5426aac9255205e9533cdd7b4235d518	
Affected Version(s): From (including) 2.6.15 Up to (excluding) 4.19.321					
Double Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: scsi: aacraid: Fix double-free on probe failure aac_probe_one() calls hardware-specific init functions through the aac_driver_ident::init pointer, all of which eventually call down to aac_init_adapter(). If aac_init_adapter() fails after allocating memory for aac_dev::queues,	https://git.kernel.org/stable/c/4b540ec7c0045c2d01c4e479f34bbc8f147afa4c, https://git.kernel.org/stable/c/564e1986b00c5f05d75342f8407f75f0a17b94df, https://git.kernel.org/stable/c/60962c3d8e18e5d8dfa16df788974dd7f35bd87a	O-LIN-LINU-190924/3264

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
			it frees the memory but does not clear that member. After the hardware-specific init function returns an error, aac_probe_one() goes down an error path that frees the memory pointed to by aac_dev::queues, resulting.in a double-free. **CVE ID: CVE-2024-46673**		
Affected Version(s): From (including) 2.6.27 Up to (excluding) 4.19.321					
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mmc: mmc_test: Fix NULL dereference on allocation failure If the "test->highmem = alloc_pages()" allocation fails then calling __free_pages(test->highmem) will result in a NULL dereference. Also change the error code to -ENOMEM	https://git.kernel.org/stable/c/2b507b03991f44dfb202fc2a82c9874d1b1f0c06, https://git.kernel.org/stable/c/3b4e76ceae5b5a46c968bd952f551ce173809f63, https://git.kernel.org/stable/c/9b9ba386d7bfdbc38445932c90fa9444c0524bea	O-LIN-LINU-190924/3265

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
			instead of returning success. **CVE ID: CVE-2024-45028**		
Affected Version(s): From (including) 2.6.32 Up to (excluding) 4.19.321					
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent UAF in ip6_send_skb() syzbot reported an UAF in ip6_send_skb() [1] After ip6_local_out() has returned, we no longer can safely dereference rt, unless we hold rcu_read_lock(). A similar issue has been fixed in commit a688caa34beb ("ipv6: take rcu lock in rawv6_send_hdrinc()") Another potential issue in ip6_finish_output2() is handled in a	https://git.kernel.org/stable/c/24e93695b1239fbe4c31e224372be77f82dab69a, https://git.kernel.org/stable/c/571567e0277008459750f0728f246086b2659429, https://git.kernel.org/stable/c/9a3e55afa95ed4ac9eda112d4f918af645d72f25	O-LIN-LINU-190924/3266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			separate patch. [1] BUG: KASAN: slab-use-after-free in ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 Read of size 8 at addr ffff88806dde4858 by task syz.1.380/6530 CPU: 1 UID: 0 PID: 6530 Comm: syz.1.380 Not tainted 6.11.0-rc3-syzkaller-00306-gdf6cbc62cc9b #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/06/2024 Call Trace: <TASK> __dump_stack lib/dump_stack.c:93 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:119 print_address_desc		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ription mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x143/0x180 mm/kasan/report.c:601 ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 rawv6_push_pending_frames+0x75c/0x9e0 net/ipv6/raw.c:588 rawv6_sendmsg+0x19c7/0x23c0 net/ipv6/raw.c:926 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 sock_write_iter+0x2dd/0x400 net/socket.c:1160		

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
			do_iter_readv_writev+0x60a/0x890 vfs_writev+0x37c/0xbb0 fs/read_write.c:971 do_writev+0x1b1/0x350 fs/read_write.c:1018 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f936bf79e79 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 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 a8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f936cd7f038 EFLAGS:		

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
			00000246 ORIG_RAX: 0000000000000014 RAX: ffffffffffffffda RBX: 00007f936c115f80 RCX: 00007f936bf79e79 RDX: 0000000000000001 RSI: 0000000020000040 RDI: 0000000000000004 RBP: 00007f936bfe7916 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000000 R14: 00007f936c115f80 R15: 00007fff2860a7a8 </TASK> Allocated by task 6530:		

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
			kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 unpoison_slab_object mm/kasan/common.c:312 [inline] __kasan_slab_alloc+0x66/0x80 mm/kasan/common.c:338 kasan_slab_alloc include/linux/kasan.h:201 [inline] slab_post_alloc_hook mm/slub.c:3988 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_noprof+0x135/0x2a0 mm/slub.c:4044 dst_alloc+0x12b/0x190 net/core/dst.c:89 ip6_blackhole_route+0x59/0x340 net/ipv6/route.c:2670		

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
			make_blackhole net/xfrm/xfrm_policy.c:3120 [inline] xfrm_lookup_route+0xd1/0x1c0 net/xfrm/xfrm_policy.c:3313 ip6_dst_lookup_flow+0x13e/0x180 net/ipv6/ip6_output.c:1257 rawv6_sendmsg+0x1283/0x23c0 net/ipv6/raw.c:898 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 ___sys_sendmsg+0x525/0x7d0 net/socket.c:2597 ___sys_sendmsg net/socket.c:2651 [inline] __sys_sendmsg+0x2b0/0x3a0 net/socket.c:2680 do_syscall_x64 arch/x86/entry/common.c:52 [inline]		

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
			do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 45: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 kasan_save_free_info+0x40/0x50 mm/kasan/generic.c:579 poison_slab_object+0xe0/0x150 mm/kasan/common.c:240 __kasan_slab_free+0x37/0x60 mm/kasan/common.c:256 kasan_slab_free include/linux/kasan.h:184 [inline] slab_free_hook mm/slub.c:2252 [inline]		

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
			slab_free mm/slub.c:4473 [inline] kmem_cache_free+0x145/0x350 mm/slub.c:4548 dst_destroy+0x2ac/0x460 net/core/dst.c:124 rcu_do_batch kernel/rcu/tree.c:2569 [inline] rcu_core+0xafd/0x1830 kernel/rcu/tree. ---truncated--- **CVE ID: CVE-2024-44987**		
Affected Version(s): From (including) 2.6.34 Up to (excluding) 4.19.321					
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: memcg_write_event_control(): fix a user-triggerable oops we are *not* guaranteed that anything past the terminating NUL is mapped (let alone initialized	https://git.kernel.org/stable/c/046667c4d3196938e992fba0dfcde570aa85cd0e, https://git.kernel.org/stable/c/0fbe2a72e853a1052abe9bc2b7df8ddb102da227, https://git.kernel.org/stable/c/1b37ec85ad95b612307627758c6018cd9d92cca8	O-LIN-LINU-190924/3267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with anything sane). **CVE ID: CVE-2024-45021**		
Affected Version(s): From (including) 2.6.36 Up to (excluding) 4.19.321					
Improper Initialization	02-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fuse: Initialize beyond-EOF page contents before setting uptodate fuse_notify_store(), unlike fuse_do_readpage(), does not enable page zeroing (because it can be used to change partial page contents). So fuse_notify_store() must be more careful to fully initialize page contents (including parts of the page that are beyond end-of-file) before marking the page uptodate. The current code can leave beyond-	https://git.kernel.org/stable/c/18a067240817bee8a9360539af5d79a4bf5398a5, https://git.kernel.org/stable/c/33168db352c7b56ae18aa55c2cae1a1c5905d30e, https://git.kernel.org/stable/c/3c0da3d163eb32f1f91891efaade027fa9b245b9	O-LIN-LINU-190924/3268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EOF page contents uninitialized, which makes these uninitialized page contents visible to userspace via mmap(). This is an information leak, but only affects systems which do not enable init-on-alloc (via CONFIG_INIT_ON_ALLOC_DEFAULT_ON=y or the corresponding kernel command line parameter). **CVE ID: CVE-2024-44947**		
Affected Version(s): From (including) 3.18 Up to (excluding) 4.19.321					
Use After Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: dwc3: st: fix probed platform device ref count on probe error path The probe function never performs any paltform device allocation, thus error path "undo_platform_de	https://git.kernel.org/stable/c/060f41243ad7f6f5249fa7290dda0c01f723d12d, https://git.kernel.org/stable/c/1de989668708ce5875efc9d669d227212aeb9a90, https://git.kernel.org/stable/c/4c6735299540f3c82a5033d35b	O-LIN-LINU-190924/3269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v_alloc" is entirely bogus. It drops the reference count from the platform device being probed. If error path is triggered, this will lead to unbalanced device reference counts and premature release of device resources, thus possible use-after-free when releasing remaining devm-managed resources. **CVE ID: CVE-2024-46674**	e76a5c42e0fb18	
Affected Version(s): From (including) 4.11 Up to (excluding) 4.19.321					
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: pinctrl: single: fix potential NULL dereference in pcs_get_function() pinmux_generic_get_function() can return NULL and the pointer 'function' was dereferenced without checking	https://git.kernel.org/stable/c/0a2bab5ed161318f57134716acba0a30f3af191, https://git.kernel.org/stable/c/1c38a62f15e595346a1106025722869e87ffe044, https://git.kernel.org/stable/c/292151af6add3e5ab11b2e9916cffa5f52859a1f	O-LIN-LINU-190924/3270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			against NULL. Add checking of pointer 'function' in pcs_get_function(). Found by code review. **CVE ID: CVE-2024-46685**		
Affected Version(s): From (including) 4.12 Up to (excluding) 4.19.321					
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: gtp: fix a potential NULL pointer dereference When sockfd_lookup() fails, gtp_encap_enable_socket() returns a NULL pointer, but its callers only check for error pointers thus miss the NULL pointer case. Fix it by returning an error pointer with the error code carried from sockfd_lookup().	https://git.kernel.org/stable/c/28c67f0f84f889fe9f4cbda8354132b20dc9212d, https://git.kernel.org/stable/c/4643b91691e969b1b9ad54bf552d7a990cfa3b87, https://git.kernel.org/stable/c/612edd35f2a3910ab1f61c1f2338889d4ba99fa2	O-LIN-LINU-190924/3271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(I found this bug during code inspection.) **CVE ID: CVE-2024-46677**		
Affected Version(s): From (including) 4.15 Up to (excluding) 4.19.295					
NULL Pointer Dereference	06-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: media: dvb-usb-v2: af9035: Fix null-ptr-deref in af9035_i2c_master_xfer In af9035_i2c_master_xfer, msg is controlled by user. When msg[i].buf is null and msg[i].len is zero, former checks on msg[i].buf would be passed. Malicious data finally reach af9035_i2c_master_xfer. If accessing msg[i].buf[0] without sanity check, null ptr deref would happen. We add check on msg[i].len to prevent crash. Similar commit:	https://git.kernel.org/stable/c/0143f282b15f7cedc0392ea10050fb6000fd16e6, https://git.kernel.org/stable/c/41b7181a40af84448a2b144fb02d8bf32b7e9a23, https://git.kernel.org/stable/c/6c01ef65de0b321b2db1ef9abf8f1d15862b937e	O-LIN-LINU-190924/3272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commit 0ed554fd769a ("media: dvb-usb: az6027: fix null-ptr-deref in az6027_i2c_xfer()") **CVE ID: CVE-2023-52915**		
Affected Version(s): From (including) 4.15 Up to (excluding) 4.19.321					
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: xhci: Fix Panther point NULL pointer deref at full-speed re-enumeration re-enumerating full-speed devices after a failed address device command can trigger a NULL pointer dereference. Full-speed devices may need to reconfigure the endpoint 0 Max Packet Size value during enumeration. Usb core calls usb_ep0_reinit() in this case,	https://git.kernel.org/stable/c/0f0654318e25b2c185e245ba4a591e42fabb5e59, https://git.kernel.org/stable/c/365ef7c4277fdd781a695c3553fa157d622d805d, https://git.kernel.org/stable/c/5ad898ae82412f8a689d59829804bff2999dd0ea	O-LIN-LINU-190924/3273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which ends up calling xhci_configure_endpoint(). On Panther point xHC the xhci_configure_endpoint() function will additionally check and reserve bandwidth in software. Other hosts do this in hardware If xHC address device command fails then a new xhci_virt_device structure is allocated as part of re-enabling the slot, but the bandwidth table pointers are not set up properly here. This triggers the NULL pointer dereference the next time usb_ep0_reinit() is called and xhci_configure_endpoint() tries to check and reserve bandwidth		

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
			[46710.713538] usb 3-1: new full-speed USB device number 5 using xhci_hcd [46710.713699] usb 3-1: Device not responding to setup address. [46710.917684] usb 3-1: Device not responding to setup address. [46711.125536] usb 3-1: device not accepting address 5, error -71 [46711.125594] BUG: kernel NULL pointer dereference, address: 0000000000000008 [46711.125600] #PF: supervisor read access in kernel mode [46711.125603] #PF: error_code(0x0000) - not-present page [46711.125606] PGD 0 P4D 0 [46711.125610] Oops: Oops: 0000 [#1] PREEMPT SMP PTI [46711.125615] CPU: 1 PID: 25760 Comm:		

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
			kworker/1:2 Not tainted 6.10.3_2 #1 [46711.125620] Hardware name: Gigabyte Technology Co., Ltd. [46711.125623] Workqueue: usb_hub_wq hub_event [usbcore] [46711.125668] RIP: 0010:xhci_reserve_bandwidth (drivers/usb/host/xhci.c Fix this by making sure bandwidth table pointers are set up correctly after a failed address device command, and additionally by avoiding checking for bandwidth in cases like this where no actual endpoints are added or removed, i.e. only context for default control endpoint 0 is evaluated. **CVE ID: CVE-2024-45006**		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.15 Up to (excluding) 5.4.283					
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix a deadlock problem when config TC during resetting When config TC during the reset process, may cause a deadlock, the flow is as below: pf reset start | ▼ ..... setup tc | | ▼ ▼ DOWN: napi_disable() napi_disable()(skip) | | ▼ ▼ .... | | ▼ | napi_enable() | ▼	https://git.kernel.org/stable/c/195918217448a6bb7f929d6a2ffffce9f1ece1cc, https://git.kernel.org/stable/c/67492d4d105c0a6321b00c393eec96b9a7a97a16, https://git.kernel.org/stable/c/6ae2b7d63cd056f363045eb65409143e16f23ae8	O-LIN-LINU-190924/3274

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
			UINIT: netif_napi_del() | ▼ ..... | ▼ INIT: netif_napi_add() | ▼ ..... global reset start | | ▼ ▼ UP: napi_enable()(skip) ..... | | ▼ ▼ ..... napi_disable() In reset process, the driver will DOWN the port and then UINIT, in this case, the setup tc process will UP the port before UINIT, so cause the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			problem. Adds a DOWN process in UINIT to fix it. **CVE ID: CVE-2024-44995**		
Affected Version(s): From (including) 4.19 Up to (excluding) 6.6.48					
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/msm/dpu: move dpu_encoder's connector assignment to atomic_enable() For cases where the crtc's connectors_changed was set without enable/active getting toggled , there is an atomic_enable() call followed by an atomic_disable() but without an atomic_mode_set(). This results in a NULL ptr access for the dpu_encoder_get_drm_fmt() call in the atomic_enable() as the dpu_encoder's	https://git.kernel.org/stable/c/3bacf814b6a61cc683c68465f175ebd938f09c52, https://git.kernel.org/stable/c/3fb61718bcbe309279205d1cc275a6435611dc77, https://git.kernel.org/stable/c/aedf02e46eb549dac8db4821a6b9f0c6bf6e3990	O-LIN-LINU-190924/3275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connector was cleared in the atomic_disable() but not re-assigned as there was no atomic_mode_set() call. Fix the NULL ptr access by moving the assignment for atomic_enable() and also use drm_atomic_get_new_connector_for_encoder() to get the connector from the atomic_state. Patchwork: https://patchwork.freedesktop.org/patch/606729/ **CVE ID: CVE-2024-45015**		
Affected Version(s): From (including) 4.19.317 Up to (excluding) 4.19.320					
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: driver core: Fix uevent_show() vs driver detach race uevent_show() wants to de-reference dev-	https://git.kernel.org/stable/c/15fffc6a5624b13b428bb1c6e9088e32a55eb82c, https://git.kernel.org/stable/c/49ea4e0d862632d51667da5e7a9c88a560e9c5a1, https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>driver->name. There is no clean way for a device attribute to de-reference dev->driver unless that attribute is defined via (struct device_driver).dev_groups. Instead, the anti-pattern of taking the device_lock() in the attribute handler risks deadlocks with code paths that remove device attributes while holding the lock. This deadlock is typically invisible to lockdep given the device_lock() is marked lockdep_set_novalidate_class(), but some subsystems allocate a local lockdep key for @dev->mutex to reveal reports of the form: ==========	4a7c2a8387524942171037e70b80e969c3b5c05b	

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
			========== WARNING: possible circular locking dependency detected 6.10.0-rc7+ #275 Tainted: G OE N ---------- modprobe/2374 is trying to acquire lock: ffff8c2270070de0 (kn->active#6){++++}-{0:0}, at: __kernfs_remove+0xde/0x220 but task is already holding lock: ffff8c22016e88f8 (&cxl_root_key){+.+.}-{3:3}, at: device_release_driver_internal+0x39/0x210 which lock already depends on the new lock. the existing dependency chain (in reverse order) is:		

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
			-> #1 (&cxl_root_key){+.+.}-{3:3}: __mutex_lock+0x99/0xc30 uevent_show+0xac/0x130 dev_attr_show+0x18/0x40 sysfs_kf_seq_show+0xac/0xf0 seq_read_iter+0x110/0x450 vfs_read+0x25b/0x340 ksys_read+0x67/0xf0 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e -> #0 (kn->active#6){++++}-{0:0}: __lock_acquire+0x121a/0x1fa0		

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
			lock_acquire+0xd6/0x2e0 kernfs_drain+0x1e9/0x200 __kernfs_remove+0xde/0x220 kernfs_remove_by_name_ns+0x5e/0xa0 device_del+0x168/0x410 device_unregister+0x13/0x60 devres_release_all+0xb8/0x110 device_unbind_cleanup+0xe/0x70 device_release_driver_internal+0x1c7/0x210 driver_detach+0x47/0x90 bus_remove_driver+0x6c/0xf0 cxl_acpi_exit+0xc/0x11 [cxl_acpi] __do_sys_delete_mo		

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
			dule.isra.0+0x181/0x260 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e The observation though is that driver objects are typically much longer lived than device objects. It is reasonable to perform lockless de-reference of a @driver pointer even if it is racing detach from a device. Given the infrequency of driver unregistration, use synchronize_rcu() in module_remove_driver() to close any potential races. It is potentially overkill to suffer synchronize_rcu() just to handle the rare module removal racing		

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
			uevent_show() event. Thanks to Tetsuo Handa for the debug analysis of the syzbot report [1]. **CVE ID: CVE-2024-44952**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.257					
NULL Pointer Dereference	06-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: media: dvb-usb-v2: af9035: Fix null-ptr-deref in af9035_i2c_master_xfer In af9035_i2c_master_xfer, msg is controlled by user. When msg[i].buf is null and msg[i].len is zero, former checks on msg[i].buf would be passed. Malicious data finally reach af9035_i2c_master_xfer. If accessing msg[i].buf[0] without sanity check, null ptr deref would happen.	https://git.kernel.org/stable/c/0143f282b15f7cedc0392ea10050fb6000fd16e6, https://git.kernel.org/stable/c/41b7181a40af84448a2b144fb02d8bf32b7e9a23, https://git.kernel.org/stable/c/6c01ef65de0b321b2db1ef9abf8f1d15862b937e	O-LIN-LINU-190924/3277

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
			We add check on msg[i].len to prevent crash. Similar commit: commit 0ed554fd769a ("media: dvb-usb: az6027: fix null-ptr-deref in az6027_i2c_xfer()") **CVE ID: CVE-2023-52915**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.283					
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent UAF in ip6_send_skb() syzbot reported an UAF in ip6_send_skb() [1] After ip6_local_out() has returned, we no longer can safely dereference rt, unless we hold rcu_read_lock(). A similar issue has been fixed in commit	https://git.kernel.org/stable/c/24e93695b1239fbe4c31e224372be77f82dab69a, https://git.kernel.org/stable/c/571567e0277008459750f0728f246086b2659429, https://git.kernel.org/stable/c/9a3e55afa95ed4ac9eda112d4f918af645d72f25	O-LIN-LINU-190924/3278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a688caa34beb ("ipv6: take rcu lock in rawv6_send_hdrinc()") Another potential issue in ip6_finish_output2() is handled in a separate patch. [1] BUG: KASAN: slab-use-after-free in ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 Read of size 8 at addr ffff88806dde4858 by task syz.1.380/6530 CPU: 1 UID: 0 PID: 6530 Comm: syz.1.380 Not tainted 6.11.0-rc3-syzkaller-00306-gdf6cbc62cc9b #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/06/2024 Call Trace: <TASK>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__dump_stack lib/dump_stack.c:93 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:119 print_address_description mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x143/0x180 mm/kasan/report.c:601 ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 rawv6_push_pending_frames+0x75c/0x9e0 net/ipv6/raw.c:588 rawv6_sendmsg+0x19c7/0x23c0 net/ipv6/raw.c:926 sock_sendmsg_nos		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 sock_write_iter+0x2dd/0x400 net/socket.c:1160 do_iter_readv_writev+0x60a/0x890 vfs_writev+0x37c/0xbb0 fs/read_write.c:971 do_writev+0x1b1/0x350 fs/read_write.c:1018 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f936bf79e79 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 48 89		

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
			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 a8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f936cd7f038 EFLAGS: 00000246 ORIG_RAX: 0000000000000014 RAX: ffffffffffffffda RBX: 00007f936c115f80 RCX: 00007f936bf79e79 RDX: 0000000000000001 RSI: 0000000020000040 RDI: 0000000000000004 RBP: 00007f936bfe7916 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000000		

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 R14: 00007f936c115f80 R15: 00007fff2860a7a8 </TASK> Allocated by task 6530: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 unpoison_slab_object mm/kasan/common.c:312 [inline] __kasan_slab_alloc+0x66/0x80 mm/kasan/common.c:338 kasan_slab_alloc include/linux/kasan.h:201 [inline] slab_post_alloc_hook mm/slub.c:3988 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_noprof+0x135/0x2a0 mm/slub.c:4044		

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
			dst_alloc+0x12b/0x190 net/core/dst.c:89 ip6_blackhole_route+0x59/0x340 net/ipv6/route.c:2670 make_blackhole net/xfrm/xfrm_policy.c:3120 [inline] xfrm_lookup_route+0xd1/0x1c0 net/xfrm/xfrm_policy.c:3313 ip6_dst_lookup_flow+0x13e/0x180 net/ipv6/ip6_output.c:1257 rawv6_sendmsg+0x1283/0x23c0 net/ipv6/raw.c:898 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 ___sys_sendmsg+0x525/0x7d0 net/socket.c:2597		

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
			___sys_sendmsg net/socket.c:2651 [inline] __sys_sendmsg+0x2b0/0x3a0 net/socket.c:2680 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 45: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 kasan_save_free_info+0x40/0x50 mm/kasan/generic.c:579 poison_slab_object+0xe0/0x150 mm/kasan/common.c:240		

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
			__kasan_slab_free+0x37/0x60 mm/kasan/common.c:256 kasan_slab_free include/linux/kasan.h:184 [inline] slab_free_hook mm/slub.c:2252 [inline] slab_free mm/slub.c:4473 [inline] kmem_cache_free+0x145/0x350 mm/slub.c:4548 dst_destroy+0x2ac/0x460 net/core/dst.c:124 rcu_do_batch kernel/rcu/tree.c:2569 [inline] rcu_core+0xafd/0x1830 kernel/rcu/tree. ---truncated--- **CVE ID: CVE-2024-44987**		
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: atm: idt77252: prevent use after	https://git.kernel.org/stable/c/09e086a5f72ea27c758b3f3b419a69000c32adc1, https://git.kernel.org/stable/c/1cece837e387c	O-LIN-LINU-190924/3279

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
			free in dequeue_rx() We can't dereference "skb" after calling vcc->push() because the skb is released. **CVE ID: CVE-2024-44998**	039225f19028df255df87a97c0d, https://git.kernel.org/stable/c/24cf390a5426aac9255205e9533cdd7b4235d518	
Double Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: scsi: aacraid: Fix double-free on probe failure aac_probe_one() calls hardware-specific init functions through the aac_driver_ident::init pointer, all of which eventually call down to aac_init_adapter(). If aac_init_adapter() fails after allocating memory for aac_dev::queues, it frees the memory but does not clear that member.	https://git.kernel.org/stable/c/4b540ec7c0045c2d01c4e479f34bbc8f147afa4c, https://git.kernel.org/stable/c/564e1986b00c5f05d75342f8407f75f0a17b94df, https://git.kernel.org/stable/c/60962c3d8e18e5d8dfa16df788974dd7f35bd87a	O-LIN-LINU-190924/3280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			After the hardware-specific init function returns an error, aac_probe_one() goes down an error path that frees the memory pointed to by aac_dev::queues, resulting.in a double-free. **CVE ID: CVE-2024-46673**		
Use After Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: dwc3: st: fix probed platform device ref count on probe error path The probe function never performs any paltform device allocation, thus error path "undo_platform_dev_alloc" is entirely bogus. It drops the reference count from the platform device being probed. If error path is triggered, this will lead to unbalanced	https://git.kernel.org/stable/c/060f41243ad7f6f5249fa7290dda0c01f723d12d, https://git.kernel.org/stable/c/1de989668708ce5875efc9d669d227212aeb9a90, https://git.kernel.org/stable/c/4c6735299540f3c82a5033d35be76a5c42e0fb18	O-LIN-LINU-190924/3281

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
			device reference counts and premature release of device resources, thus possible use-after-free when releasing remaining devm-managed resources. **CVE ID: CVE-2024-46674**		
Use of Uninitialized Resource	04-Sep-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: gtp: pull network headers in gtp_dev_xmit() syzbot/KMSAN reported use of uninit-value in get_dev_xmit() [1] We must make sure the IPv4 or Ipv6 header is pulled in skb->head before accessing fields in them. Use pskb_inet_may_pull() to fix this issue. [1]	https://git.kernel.org/stable/c/137d565ab89ce3584503b443bc9e00d44f482593, https://git.kernel.org/stable/c/1f6b62392453d8f36685d19b761307a8c5617ac1, https://git.kernel.org/stable/c/34ba4f29f3d9eb52dee37512059efb2afd7e966f	O-LIN-LINU-190924/3282

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
			BUG: KMSAN: uninit-value in ipv6_pdp_find drivers/net/gtp.c:220 [inline] BUG: KMSAN: uninit-value in gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] BUG: KMSAN: uninit-value in gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281 ipv6_pdp_find drivers/net/gtp.c:220 [inline] gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281 __netdev_start_xmit include/linux/netdevice.h:4913 [inline] netdev_start_xmit include/linux/netdevice.h:4922 [inline] xmit_one net/core/dev.c:3580 [inline] dev_hard_start_xmi		

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
			t+0x247/0xa20 net/core/dev.c:3596 __dev_queue_xmit+0x358c/0x5610 net/core/dev.c:4423 dev_queue_xmit include/linux/netdevice.h:3105 [inline] packet_xmit+0x9c/0x6c0 net/packet/af_packet.c:276 packet_snd net/packet/af_packet.c:3145 [inline] packet_sendmsg+0x90e3/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline]		

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
			__se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3994 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_node_noprof+0x6bf/0xb80 mm/slub.c:4080		

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
			kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:583 __alloc_skb+0x363/0x7b0 net/core/skbuff.c:674 alloc_skb include/linux/skbuff.h:1320 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6526 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2815 packet_alloc_skb net/packet/af_packet.c:2994 [inline] packet_snd net/packet/af_packet.c:3088 [inline] packet_sendmsg+0x749c/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+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
			x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f CPU: 0 UID: 0 PID: 7115 Comm: syz.1.515 Not tainted 6.11.0-rc1-		

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
			syzkaller-00043-g94ede2a3e913 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 **CVE ID: CVE-2024-44999**		
Improper Initialization	02-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fuse: Initialize beyond-EOF page contents before setting uptodate fuse_notify_store(), unlike fuse_do_readpage(), does not enable page zeroing (because it can be used to change partial page contents). So fuse_notify_store() must be more careful to fully initialize page contents (including parts of the page that are beyond end-of-file)	https://git.kernel.org/stable/c/18a067240817bee8a9360539af5d79a4bf5398a5, https://git.kernel.org/stable/c/33168db352c7b56ae18aa55c2cae1a1c5905d30e, https://git.kernel.org/stable/c/3c0da3d163eb32f1f91891efaade027fa9b245b9	O-LIN-LINU-190924/3283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before marking the page uptodate. The current code can leave beyond-EOF page contents uninitialized, which makes these uninitialized page contents visible to userspace via mmap(). This is an information leak, but only affects systems which do not enable init-on-alloc (via CONFIG_INIT_ON_ALLOC_DEFAULT_ON=y or the corresponding kernel command line parameter). **CVE ID: CVE-2024-44947**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: xhci: Fix Panther point NULL pointer deref at full-speed re-enumeration re-enumerating full-speed devices	https://git.kernel.org/stable/c/0f0654318e25b2c185e245ba4a591e42fabb5e59, https://git.kernel.org/stable/c/365ef7c4277fdd781a695c3553fa157d622d805d, https://git.kern	O-LIN-LINU-190924/3284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			after a failed address device command can trigger a NULL pointer dereference. Full-speed devices may need to reconfigure the endpoint 0 Max Packet Size value during enumeration. Usb core calls usb_ep0_reinit() in this case, which ends up calling xhci_configure_endpoint(). On Panther point xHC the xhci_configure_endpoint() function will additionally check and reserve bandwidth in software. Other hosts do this in hardware If xHC address device command fails then a new xhci_virt_device structure	el.org/stable/c/5ad898ae82412f8a689d59829804bff2999dd0ea	

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
			is allocated as part of re-enabling the slot, but the bandwidth table pointers are not set up properly here. This triggers the NULL pointer dereference the next time usb_ep0_reinit() is called and xhci_configure_endpoint() tries to check and reserve bandwidth [46710.713538] usb 3-1: new full-speed USB device number 5 using xhci_hcd [46710.713699] usb 3-1: Device not responding to setup address. [46710.917684] usb 3-1: Device not responding to setup address. [46711.125536] usb 3-1: device not accepting address 5, error -71 [46711.125594] BUG: kernel NULL pointer dereference, address:		

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
			0000000000000008 [46711.125600] #PF: supervisor read access in kernel mode [46711.125603] #PF: error_code(0x0000) - not-present page [46711.125606] PGD 0 P4D 0 [46711.125610] Oops: Oops: 0000 [#1] PREEMPT SMP PTI [46711.125615] CPU: 1 PID: 25760 Comm: kworker/1:2 Not tainted 6.10.3_2 #1 [46711.125620] Hardware name: Gigabyte Technology Co., Ltd. [46711.125623] Workqueue: usb_hub_wq hub_event [usbcore] [46711.125668] RIP: 0010:xhci_reserve_bandwidth (drivers/usb/host/xhci.c Fix this by making sure bandwidth		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			table pointers are set up correctly after a failed address device command, and additionally by avoiding checking for bandwidth in cases like this where no actual endpoints are added or removed, i.e. only context for default control endpoint 0 is evaluated. **CVE ID: CVE-2024-45006**		
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: memcg_write_event_control(): fix a user-triggerable oops we are *not* guaranteed that anything past the terminating NUL is mapped (let alone initialized with anything sane). **CVE ID: CVE-2024-45021**	https://git.kernel.org/stable/c/046667c4d3196938e992fba0dfcde570aa85cd0e, https://git.kernel.org/stable/c/0fbe2a72e853a1052abe9bc2b7df8ddb102da227, https://git.kernel.org/stable/c/1b37ec85ad95b612307627758c6018cd9d92cca8	O-LIN-LINU-190924/3285

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
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fix bitmap corruption on close_range() with CLOSE_RANGE_UNSHARE copy_fd_bitmaps(new, old, count) is expected to copy the first count/BITS_PER_LONG bits from old->full_fds_bits[] and fill the rest with zeroes. What it does is copying enough words (BITS_TO_LONGS(count/BITS_PER_LONG)), then memsets the rest. That works fine, *if* all bits past the cutoff point are clear. Otherwise we are risking garbage from the last word we'd copied. For most of the callers that is true - expand_fdtable() has	https://git.kernel.org/stable/c/5053581fe5dfb09b58c65dd8462bf5dea71f41ff, https://git.kernel.org/stable/c/8cad3b2b3ab81ca55f37405ffd1315bcc2948058, https://git.kernel.org/stable/c/9a2fa1472083580b6c66bdaf291f591e1170123a	O-LIN-LINU-190924/3286

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
			count equal to old->max_fds, so there's no open descriptors past count, let alone fully occupied words in ->open_fds[], which is what bits in ->full_fds_bits[] correspond to. The other caller (dup_fd()) passes sane_fdtable_size(old_fdt, max_fds), which is the smallest multiple of BITS_PER_LONG that covers all opened descriptors below max_fds. In the common case (copying on fork()) max_fds is ~0U, so all opened descriptors will be below it and we are fine, by the same reasons why the call in expand_fdtable() is safe. Unfortunately, there is a case where max_fds is less than that		

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
			and where we might, indeed, end up with junk in ->full_fds_bits[] - close_range(from, to, CLOSE_RANGE_UNSHARE) with * descriptor table being currently shared * 'to' being above the current capacity of descriptor table * 'from' being just under some chunk of opened descriptors. In that case we end up with observably wrong behaviour - e.g. spawn a child with CLONE_FILES, get all descriptors in range 0..127 open, then close_range(64, ~0U, CLOSE_RANGE_UNSHARE) and watch dup(0) ending up with descriptor #128, despite #64 being observably not open. The minimally invasive fix would		

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
			be to deal with that in dup_fd(). If this proves to add measurable overhead, we can go that way, but let's try to fix copy_fd_bitmaps() first. * new helper: bitmap_copy_and_expand(to, from, bits_to_copy, size). * make copy_fd_bitmaps() take the bitmap size in words, rather than bits; it's 'count' argument is always a multiple of BITS_PER_LONG, so we are not losing any information, and that way we can use the same helper for all three bitmaps - compiler will see that count is a multiple of BITS_PER_LONG for the large ones, so it'll generate plain memcpy()+memset().		

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
			Reproducer added to tools/testing/selftests/core/close_range_test.c **CVE ID: CVE-2024-45025**		
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mmc: mmc_test: Fix NULL dereference on allocation failure If the "test->highmem = alloc_pages()" allocation fails then calling __free_pages(test->highmem) will result in a NULL dereference. Also change the error code to -ENOMEM instead of returning success. **CVE ID: CVE-2024-45028**	https://git.kernel.org/stable/c/2b507b03991f44dfb202fc2a82c9874d1b1f0c06, https://git.kernel.org/stable/c/3b4e76ceae5b5a46c968bd952f551ce173809f63, https://git.kernel.org/stable/c/9b9ba386d7bfdbc38445932c90fa9444c0524bea	O-LIN-LINU-190924/3287
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: gtp: fix a potential NULL pointer dereference	https://git.kernel.org/stable/c/28c67f0f84f889fe9f4cbda8354132b20dc9212d, https://git.kernel.org/stable/c/4643b91691e969b1b9ad54bf5	O-LIN-LINU-190924/3288

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
			When sockfd_lookup() fails, gtp_encap_enable_socket() returns a NULL pointer, but its callers only check for error pointers thus miss the NULL pointer case. Fix it by returning an error pointer with the error code carried from sockfd_lookup(). (I found this bug during code inspection.) **CVE ID: CVE-2024-46677**	52d7a990cfa3b87, https://git.kernel.org/stable/c/612edd35f2a3910ab1f61c1f2338889d4ba99fa2	
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: pinctrl: single: fix potential NULL dereference in pcs_get_function() pinmux_generic_get_function() can return NULL and the pointer 'function'	https://git.kernel.org/stable/c/0a2bab5ed161318f57134716accba0a30f3af191, https://git.kernel.org/stable/c/1c38a62f15e595346a1106025722869e87ffe044, https://git.kernel.org/stable/c/292151af6add3	O-LIN-LINU-190924/3289

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
			was dereferenced without checking against NULL. Add checking of pointer 'function' in pcs_get_function(). Found by code review. **CVE ID: CVE-2024-46685**	e5ab11b2e9916cffa5f52859a1f	
Affected Version(s): From (including) 4.7 Up to (excluding) 4.19.321					
Use of Uninitialized Resource	04-Sep-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: gtp: pull network headers in gtp_dev_xmit() syzbot/KMSAN reported use of uninit-value in get_dev_xmit() [1] We must make sure the IPv4 or Ipv6 header is pulled in skb->head before accessing fields in them. Use pskb_inet_may_pull() to fix this issue. [1]	https://git.kernel.org/stable/c/137d565ab89ce3584503b443bc9e00d44f482593, https://git.kernel.org/stable/c/1f6b62392453d8f36685d19b761307a8c5617ac1, https://git.kernel.org/stable/c/34ba4f29f3d9eb52dee37512059efb2afd7e966f	O-LIN-LINU-190924/3290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BUG: KMSAN: uninit-value in ipv6_pdp_find drivers/net/gtp.c:220 [inline] BUG: KMSAN: uninit-value in gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] BUG: KMSAN: uninit-value in gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281 ipv6_pdp_find drivers/net/gtp.c:220 [inline] gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281 __netdev_start_xmit include/linux/netdevice.h:4913 [inline] netdev_start_xmit include/linux/netdevice.h:4922 [inline] xmit_one net/core/dev.c:3580 [inline] dev_hard_start_xmi		

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
			t+0x247/0xa20 net/core/dev.c:3596 __dev_queue_xmit+0x358c/0x5610 net/core/dev.c:4423 dev_queue_xmit include/linux/netdevice.h:3105 [inline] packet_xmit+0x9c/0x6c0 net/packet/af_packet.c:276 packet_snd net/packet/af_packet.c:3145 [inline] packet_sendmsg+0x90e3/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline]		

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
			__se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3994 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_node_noprof+0x6bf/0xb80 mm/slub.c:4080		

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
			kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:583 __alloc_skb+0x363/0x7b0 net/core/skbuff.c:674 alloc_skb include/linux/skbuff.h:1320 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6526 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2815 packet_alloc_skb net/packet/af_packet.c:2994 [inline] packet_snd net/packet/af_packet.c:3088 [inline] packet_sendmsg+0x749c/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+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
			x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f CPU: 0 UID: 0 PID: 7115 Comm: syz.1.515 Not tainted 6.11.0-rc1-		

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
			syzkaller-00043-g94ede2a3e913 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 **CVE ID: CVE-2024-44999**		
Affected Version(s): From (including) 5.0 Up to (excluding) 5.4.283					
Use After Free	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netem: fix return value if duplicate enqueue fails There is a bug in netem_enqueue() introduced by commit 5845f706388a ("net: netem: fix skb length BUG_ON in __skb_to_sgvec") that can lead to a use-after-free. This commit made netem_enqueue() always return NET_XMIT_SUCCESS when a packet is duplicated, which can cause the	https://git.kernel.org/stable/c/0486d31dd8198e22b63a4730244b38fffce6d469, https://git.kernel.org/stable/c/52d99a69f3d556c6426048c9d481b912205919d8, https://git.kernel.org/stable/c/577d6c0619467fe90f7e8e57e45cb5bd9d36014	O-LIN-LINU-190924/3291

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
			parent qdisc's q.qlen to be mistakenly incremented. When this happens qlen_notify() may be skipped on the parent during destruction, leaving a dangling pointer for some classful qdiscs like DRR. There are two ways for the bug happen: - If the duplicated packet is dropped by rootq->enqueue() and then the original packet is also dropped. - If rootq->enqueue() sends the duplicated packet to a different qdisc and the original packet is dropped. In both cases NET_XMIT_SUCCESS is returned even though no packets are enqueued at the netem qdisc.		

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 fix is to defer the enqueue of the duplicate packet until after the original packet has been guaranteed to return NET_XMIT_SUCCESS. **CVE ID: CVE-2024-45016**		
Affected Version(s): From (including) 5.10 Up to (excluding) 5.10.224					
Missing Release of Memory after Effective Lifetime	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: dsa: bcm_sf2: Fix a possible memory leak in bcm_sf2_mdio_register() bcm_sf2_mdio_register() calls of_phy_find_device() and then phy_device_remove() in a loop to remove existing PHY devices. of_phy_find_device() eventually calls bus_find_device(), which calls get_device() on the returned struct device * to	https://git.kernel.org/stable/c/7feef10768ea71d468d9bbc1e0d14c461876768c, https://git.kernel.org/stable/c/a7d2808d67570e6acae45c2a96e0d59986888e4c, https://git.kernel.org/stable/c/b7b8d9f5e679af60c94251fd6728dde34be69a71	O-LIN-LINU-190924/3292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			increment the refcount. The current implementation does not decrement the refcount, which causes memory leak. This commit adds the missing phy_device_free() call to decrement the refcount via put_device() to balance the refcount. **CVE ID: CVE-2024-44971**		
Affected Version(s): From (including) 5.10 Up to (excluding) 5.15.167					
N/A	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: only decrement add_addr_accepted for MPJ req Adding the following warning ... WARN_ON_ONCE(msk-	https://git.kernel.org/stable/c/1c1f721375989579e46741f59523e39ec9b2a9bd, https://git.kernel.org/stable/c/2060f1efab370b496c4903b840844ecaff324c3c, https://git.kernel.org/stable/c/35b31f5549ede4070566b949781e83495906b43d	O-LIN-LINU-190924/3293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>pm.add_addr_accepted == 0) ... before decrementing the add_addr_accepted counter helped to find a bug when running the "remove single subflow" subtest from the mptcp_join.sh selftest. Removing a 'subflow' endpoint will first trigger a RM_ADDR, then the subflow closure. Before this patch, and upon the reception of the RM_ADDR, the other peer will then try to decrement this add_addr_accepted. That's not correct because the attached subflows have not been created upon the reception of an ADD_ADDR. A way to solve that is to decrement the counter only if the attached		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			subflow was an MP_JOIN to a remote id that was not 0, and initiated by the host receiving the RM_ADDR. **CVE ID: CVE-2024-45009**		
Affected Version(s): From (including) 5.10.221 Up to (excluding) 5.10.224					
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: driver core: Fix uevent_show() vs driver detach race uevent_show() wants to de-reference dev->driver->name. There is no clean way for a device attribute to de-reference dev->driver unless that attribute is defined via (struct device_driver).dev_groups. Instead, the anti-pattern of taking the device_lock() in the attribute handler risks deadlocks with code paths that remove device	https://git.kernel.org/stable/c/15fffc6a5624b13b428bb1c6e9088e32a55eb82c, https://git.kernel.org/stable/c/49ea4e0d862632d51667da5e7a9c88a560e9c5a1, https://git.kernel.org/stable/c/4a7c2a8387524942171037e70b80e969c3b5c05b	O-LIN-LINU-190924/3294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attributes while holding the lock. This deadlock is typically invisible to lockdep given the device_lock() is marked lockdep_set_novalidate_class(), but some subsystems allocate a local lockdep key for @dev->mutex to reveal reports of the form: ========== ========== ========== ========= WARNING: possible circular locking dependency detected 6.10.0-rc7+ #275 Tainted: G OE N --- --- --- modprobe/2374 is trying to acquire lock: ffff8c2270070de0 (kn->active#6){++++}-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			{0:0}, at: __kernfs_remove+0xde/0x220 but task is already holding lock: ffff8c22016e88f8 (&cxl_root_key){+.+.}-{3:3}, at: device_release_driver_internal+0x39/0x210 which lock already depends on the new lock. the existing dependency chain (in reverse order) is: -> #1 (&cxl_root_key){+.+.}-{3:3}: __mutex_lock+0x99/0xc30 uevent_show+0xac/0x130 dev_attr_show+0x18/0x40 sysfs_kf_seq_show+0xac/0xf0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			seq_read_iter+0x110/0x450 vfs_read+0x25b/0x340 ksys_read+0x67/0xf0 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e -> #0 (kn->active#6){++++}-{0:0}: __lock_acquire+0x121a/0x1fa0 lock_acquire+0xd6/0x2e0 kernfs_drain+0x1e9/0x200 __kernfs_remove+0xde/0x220 kernfs_remove_by_name_ns+0x5e/0xa0 device_del+0x168/0x410		

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
			device_unregister+0x13/0x60 devres_release_all+0xb8/0x110 device_unbind_cleanup+0xe/0x70 device_release_driver_internal+0x1c7/0x210 driver_detach+0x47/0x90 bus_remove_driver+0x6c/0xf0 cxl_acpi_exit+0xc/0x11 [cxl_acpi] __do_sys_delete_module.isra.0+0x181/0x260 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e The observation though is that driver objects are typically much longer		

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
			lived than device objects. It is reasonable to perform lockless de-reference of a @driver pointer even if it is racing detach from a device. Given the infrequency of driver unregistration, use synchronize_rcu() in module_remove_driver() to close any potential races. It is potentially overkill to suffer synchronize_rcu() just to handle the rare module removal racing uevent_show() event. Thanks to Tetsuo Handa for the debug analysis of the syzbot report [1]. **CVE ID: CVE-2024-44952**		
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.133					
NULL Pointer Dereference	06-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/0143f282b15f7cedc0392ea10050fb6000fd16e	O-LIN-LINU-190924/3295

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
			media: dvb-usb-v2: af9035: Fix null-ptr-deref in af9035_i2c_master_xfer In af9035_i2c_master_xfer, msg is controlled by user. When msg[i].buf is null and msg[i].len is zero, former checks on msg[i].buf would be passed. Malicious data finally reach af9035_i2c_master_xfer. If accessing msg[i].buf[0] without sanity check, null ptr deref would happen. We add check on msg[i].len to prevent crash. Similar commit: commit 0ed554fd769a ("media: dvb-usb: az6027: fix null-ptr-deref in az6027_i2c_xfer()") **CVE ID: CVE-2023-52915**	6, https://git.kernel.org/stable/c/41b7181a40af84448a2b144fb02d8bf32b7e9a23, https://git.kernel.org/stable/c/6c01ef65de0b321b2db1ef9abf8f1d15862b937e	
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.165					

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
Missing Release of Memory after Effective Lifetime	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: dsa: bcm_sf2: Fix a possible memory leak in bcm_sf2_mdio_register() bcm_sf2_mdio_register() calls of_phy_find_device() and then phy_device_remove() in a loop to remove existing PHY devices. of_phy_find_device() eventually calls bus_find_device(), which calls get_device() on the returned struct device * to increment the refcount. The current implementation does not decrement the refcount, which causes memory leak. This commit adds the missing phy_device_free() call to decrement the	https://git.kernel.org/stable/c/7feef10768ea71d468d9bbc1e0d14c461876768c, https://git.kernel.org/stable/c/a7d2808d67570e6acae45c2a96e0d59986888e4c, https://git.kernel.org/stable/c/b7b8d9f5e679af60c94251fd6728dde34be69a71	O-LIN-LINU-190924/3296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			refcount via put_device() to balance the refcount. **CVE ID: CVE-2024-44971**		
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.166					
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent UAF in ip6_send_skb() syzbot reported an UAF in ip6_send_skb() [1] After ip6_local_out() has returned, we no longer can safely dereference rt, unless we hold rcu_read_lock(). A similar issue has been fixed in commit a688caa34beb ("ipv6: take rcu lock in rawv6_send_hdrinc()") Another potential issue in	https://git.kernel.org/stable/c/24e93695b1239fbe4c31e224372be77f82dab69a, https://git.kernel.org/stable/c/571567e0277008459750f0728f24608b2659429, https://git.kernel.org/stable/c/9a3e55afa95ed4ac9eda112d4f918af645d72f25	O-LIN-LINU-190924/3297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ip6_finish_output2() is handled in a separate patch. [1] BUG: KASAN: slab-use-after-free in ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 Read of size 8 at addr ffff88806dde4858 by task syz.1.380/6530 CPU: 1 UID: 0 PID: 6530 Comm: syz.1.380 Not tainted 6.11.0-rc3-syzkaller-00306-gdf6cbc62cc9b #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/06/2024 Call Trace: <TASK> __dump_stack lib/dump_stack.c:93 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:119		

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
			print_address_description mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x143/0x180 mm/kasan/report.c:601 ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 rawv6_push_pending_frames+0x75c/0x9e0 net/ipv6/raw.c:588 rawv6_sendmsg+0x19c7/0x23c0 net/ipv6/raw.c:926 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 sock_write_iter+0x		

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
			2dd/0x400 net/socket.c:1160 do_iter_readv_writev+0x60a/0x890 vfs_writev+0x37c/0xbb0 fs/read_write.c:971 do_writev+0x1b1/0x350 fs/read_write.c:1018 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f936bf79e79 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 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 a8 ff ff ff f7 d8 64 89 01 48		

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
			RSP: 002b:00007f936cd7f038 EFLAGS: 00000246 ORIG_RAX: 0000000000000014 RAX: ffffffffffffffda RBX: 00007f936c115f80 RCX: 00007f936bf79e79 RDX: 0000000000000001 RSI: 0000000020000040 RDI: 0000000000000004 RBP: 00007f936bfe7916 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000000 R14: 00007f936c115f80 R15: 00007fff2860a7a8 </TASK>		

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
			Allocated by task 6530: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 unpoison_slab_object mm/kasan/common.c:312 [inline] __kasan_slab_alloc+0x66/0x80 mm/kasan/common.c:338 kasan_slab_alloc include/linux/kasan.h:201 [inline] slab_post_alloc_hook mm/slub.c:3988 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_noprof+0x135/0x2a0 mm/slub.c:4044 dst_alloc+0x12b/0x190 net/core/dst.c:89 ip6_blackhole_route+0x59/0x340		

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
			net/ipv6/route.c:2670 make_blackhole net/xfrm/xfrm_policy.c:3120 [inline] xfrm_lookup_route+0xd1/0x1c0 net/xfrm/xfrm_policy.c:3313 ip6_dst_lookup_flow+0x13e/0x180 net/ipv6/ip6_output.c:1257 rawv6_sendmsg+0x1283/0x23c0 net/ipv6/raw.c:898 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 ___sys_sendmsg+0x525/0x7d0 net/socket.c:2597 __sys_sendmsg net/socket.c:2651 [inline] __sys_sendmsg+0x2b0/0x3a0 net/socket.c:2680		

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
			do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 45: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 kasan_save_free_info+0x40/0x50 mm/kasan/generic.c:579 poison_slab_object+0xe0/0x150 mm/kasan/common.c:240 __kasan_slab_free+0x37/0x60 mm/kasan/common.c:256 kasan_slab_free include/linux/kasan.h:184 [inline]		

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
			slab_free_hook mm/slub.c:2252 [inline] slab_free mm/slub.c:4473 [inline] kmem_cache_free+0x145/0x350 mm/slub.c:4548 dst_destroy+0x2ac/0x460 net/core/dst.c:124 rcu_do_batch kernel/rcu/tree.c:2569 [inline] rcu_core+0xafd/0x1830 kernel/rcu/tree. ---truncated--- **CVE ID: CVE-2024-44987**		
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: atm: idt77252: prevent use after free in dequeue_rx() We can't dereference "skb" after calling vcc->push() because the skb	https://git.kernel.org/stable/c/09e086a5f72ea27c758b3f3b419a69000c32adc1, https://git.kernel.org/stable/c/1cece837e387c039225f19028df255df87a97c0d, https://git.kernel.org/stable/c/24cf390a5426aac9255205e953	O-LIN-LINU-190924/3298

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
			is released. **CVE ID: CVE-2024-44998**	3cdd7b4235d518	
Out-of-bounds Write	11-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: s390/dasd: fix error recovery leading to data corruption on ESE devices Extent Space Efficient (ESE) or thin provisioned volumes need to be formatted on demand during usual IO processing. The dasd_ese_needs_format function checks for error codes that signal the non existence of a proper track format. The check for incorrect length is to imprecise since other error cases leading to transport of insufficient data	https://git.kernel.org/stable/c/0a228896a1b3654cd461ff654f6a64e97a9c3246, https://git.kernel.org/stable/c/19f60a55b2fda49bc4f6134a5f6356ef62ee69d8, https://git.kernel.org/stable/c/5d4a304338daf83ace2887aaacafd66fe99ed5cc	O-LIN-LINU-190924/3299

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
			also have this flag set. This might lead to data corruption in certain error cases for example during a storage server warmstart. Fix by removing the check for incorrect length and replacing by explicitly checking for invalid track format in transport mode. Also remove the check for file protected since this is not a valid ESE handling case. **CVE ID: CVE-2024-45026**		
Double Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: scsi: aacraid: Fix double-free on probe failure aac_probe_one() calls hardware-specific init functions through the	https://git.kernel.org/stable/c/4b540ec7c0045c2d01c4e479f34bbc8f147afa4c, https://git.kernel.org/stable/c/564e1986b00c5f05d75342f8407f75f0a17b94df, https://git.kernel.org/stable/c/60962c3d8e18e5d8dfa16df788	O-LIN-LINU-190924/3300

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
			aac_driver_ident::init pointer, all of which eventually call down to aac_init_adapter(). If aac_init_adapter() fails after allocating memory for aac_dev::queues, it frees the memory but does not clear that member. After the hardware-specific init function returns an error, aac_probe_one() goes down an error path that frees the memory pointed to by aac_dev::queues, resulting.in a double-free. **CVE ID: CVE-2024-46673**	974dd7f35bd87a	
Use After Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: dwc3: st: fix probed platform device ref count on probe error path	https://git.kernel.org/stable/c/060f41243ad7f6f5249fa7290dda0c01f723d12d, https://git.kernel.org/stable/c/1de989668708ce5875efc9d669d227212aeb9a90, https://git.kern	O-LIN-LINU-190924/3301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The probe function never performs any paltform device allocation, thus error path "undo_platform_dev_alloc" is entirely bogus. It drops the reference count from the platform device being probed. If error path is triggered, this will lead to unbalanced device reference counts and premature release of device resources, thus possible use-after-free when releasing remaining devm-managed resources. **CVE ID: CVE-2024-46674**	el.org/stable/c/4c6735299540f3c82a5033d35be76a5c42e0fb18	
Use of Uninitialized Resource	04-Sep-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: gtp: pull network headers in gtp_dev_xmit() syzbot/KMSAN reported use of uninit-value in get_dev_xmit() [1]	https://git.kernel.org/stable/c/137d565ab89ce3584503b443bc9e00d44f482593, https://git.kernel.org/stable/c/1f6b62392453d8f36685d19b761307a8c5617ac1, https://git.kernel.org/stable/c/34ba4f29f3d9e	O-LIN-LINU-190924/3302

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
			We must make sure the IPv4 or Ipv6 header is pulled in skb->head before accessing fields in them. Use pskb_inet_may_pull() to fix this issue. [1] BUG: KMSAN: uninit-value in ipv6_pdp_find drivers/net/gtp.c:220 [inline] BUG: KMSAN: uninit-value in gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] BUG: KMSAN: uninit-value in gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281 ipv6_pdp_find drivers/net/gtp.c:220 [inline] gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281	b52dee37512059efb2afd7e966f	

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
			__netdev_start_xmit include/linux/netdevice.h:4913 [inline] netdev_start_xmit include/linux/netdevice.h:4922 [inline] xmit_one net/core/dev.c:3580 [inline] dev_hard_start_xmit+0x247/0xa20 net/core/dev.c:3596 __dev_queue_xmit+0x358c/0x5610 net/core/dev.c:4423 dev_queue_xmit include/linux/netdevice.h:3105 [inline] packet_xmit+0x9c/0x6c0 net/packet/af_packet.c:276 packet_snd net/packet/af_packet.c:3145 [inline] packet_sendmsg+0x90e3/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nos		

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
			ec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f		

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
			Uninit was created at: slab_post_alloc_hook mm/slub.c:3994 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_node_noprof+0x6bf/0xb80 mm/slub.c:4080 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:583 __alloc_skb+0x363/0x7b0 net/core/skbuff.c:674 alloc_skb include/linux/skbuff.h:1320 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6526 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2815 packet_alloc_skb net/packet/af_packet.c:2994 [inline]		

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
			packet_snd net/packet/af_packet.c:3088 [inline] packet_sendmsg+0x749c/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd		

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
			/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f CPU: 0 UID: 0 PID: 7115 Comm: syz.1.515 Not tainted 6.11.0-rc1-syzkaller-00043-g94ede2a3e913 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 **CVE ID: CVE-2024-44999**		
Improper Initialization	02-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fuse: Initialize beyond-EOF page contents before setting uptodate fuse_notify_store(), unlike fuse_do_readpage(), does not enable page zeroing (because it can be used to	https://git.kernel.org/stable/c/18a067240817bee8a9360539af5d79a4bf5398a5, https://git.kernel.org/stable/c/33168db352c7b56ae18aa55c2cae1a1c5905d30e, https://git.kernel.org/stable/c/3c0da3d163eb32f1f91891efaade027fa9b245b9	O-LIN-LINU-190924/3303

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
			change partial page contents). So fuse_notify_store() must be more careful to fully initialize page contents (including parts of the page that are beyond end-of-file) before marking the page uptodate. The current code can leave beyond-EOF page contents uninitialized, which makes these uninitialized page contents visible to userspace via mmap(). This is an information leak, but only affects systems which do not enable init-on-alloc (via CONFIG_INIT_ON_ALLOC_DEFAULT_ON=y or the corresponding kernel command line parameter). **CVE ID: CVE-2024-44947**		

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
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bonding: fix xfrm real_dev null pointer dereference We shouldn't set real_dev to NULL because packets can be in transit and xfrm might call xdo_dev_offload_ok() in parallel. All callbacks assume real_dev is set. Example trace: kernel: BUG: unable to handle page fault for address: 0000000000001030 kernel: bond0: (slave eni0np1): making interface the new active one kernel: #PF: supervisor write access in kernel mode kernel: #PF: error_code(0x0002) - not-present page	https://git.kernel.org/stable/c/21816b696c172c19d53a30d45ee005cce246ed21, https://git.kernel.org/stable/c/2f72c6a66bcd7e0187ec085237fee5db27145294, https://git.kernel.org/stable/c/4582d4ff413a07d4ed8a4823c652dc5207760548	O-LIN-LINU-190924/3304

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
			kernel: PGD 0 P4D 0 kernel: Oops: 0002 [#1] PREEMPT SMP kernel: CPU: 4 PID: 2237 Comm: ping Not tainted 6.7.7+ #12 kernel: Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 kernel: RIP: 0010:nsim_ipsec_offload_ok+0xc/0x20 [netdevsim] kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: Code: e0 0f 0b 48 83 7f 38 00 74 de 0f 0b 48 8b 47 08 48 8b 37 48 8b 78 40 e9 b2 e5 9a d7 66 90 0f 1f 44 00 00 48 8b 86 80 02 00 00 <83> 80 30 10 00 00 01 b8 01 00 00 00 c3 0f 1f 80 00 00 00 00 0f 1f kernel: bond0: (slave eni0np1): making interface the new active one kernel: RSP: 0018:ffffabde8155		

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
			3b98 EFLAGS: 00010246 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: kernel: RAX: 0000000000000000 RBX: ffff9eb404e74900 RCX: ffff9eb403d97c60 kernel: RDX: ffffffffc090de10 RSI: ffff9eb404e74900 RDI: ffff9eb3c5de9e00 kernel: RBP: ffff9eb3c0a42000 R08: 0000000000000010 R09: 0000000000000014 kernel: R10: 7974203030303030 R11: 3030303030303030 R12: 0000000000000000 kernel: R13: ffff9eb3c5de9e00 R14: ffffabde81553cc8 R15: ffff9eb404c53000 kernel: FS: 00007f2a77a3ad0		

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(0000) GS:ffff9eb43bd00000(0000) knlGS:0000000000000000 kernel: CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 kernel: CR2: 0000000000001030 CR3: 00000001122ab000 CR4: 0000000000350ef0 kernel: bond0: (slave eni0np1): making interface the new active one kernel: Call Trace: kernel: <TASK> kernel: ? __die+0x1f/0x60 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ? page_fault_oops+0x142/0x4c0 kernel: ? do_user_addr_fault+0x65/0x670 kernel: ? kvm_read_and_reset_apf_flags+0x3b/0x50		

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
			kernel: bond0: (slave eni0np1): making interface the new active one kernel: ? exc_page_fault+0x7b/0x180 kernel: ? asm_exc_page_fault+0x22/0x30 kernel: ? nsim_bpf_uninit+0x50/0x50 [netdevsim] kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ? nsim_ipsec_offload_ok+0xc/0x20 [netdevsim] kernel: bond0: (slave eni0np1): making interface the new active one kernel: bond_ipsec_offload_ok+0x7b/0x90 [bonding] kernel: xfrm_output+0x61/0x3b0 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ip_push_pending_frames+0x56/0x80		

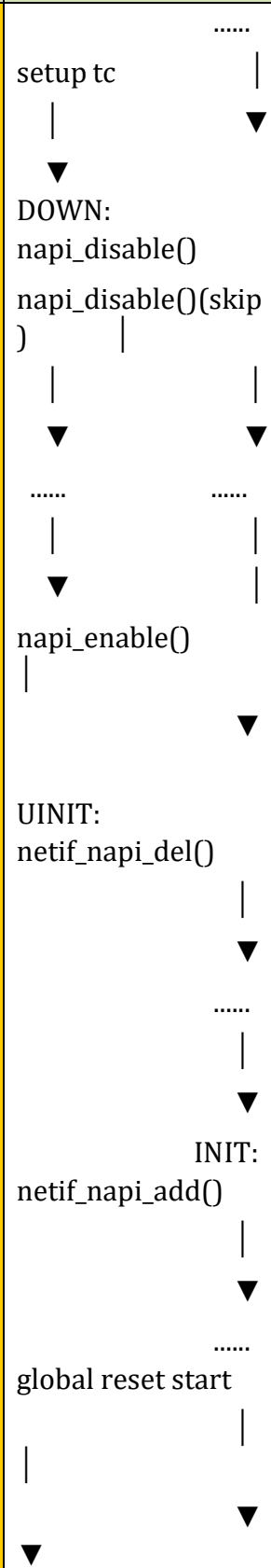
CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-44989		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bonding: fix null pointer deref in bond_ipsec_offload_ok We must check if there is an active slave before dereferencing the pointer. **CVE ID: CVE-2024-44990**	https://git.kernel.org/stable/c/0707260a18312bbcd2a566858e4e3692d0a29e3f6, https://git.kernel.org/stable/c/2f5bdd68c1ce64bda6bef4d361a3de23b04ccd59, https://git.kernel.org/stable/c/32a0173600c63aadaf2103bf02f074982e8602ab	O-LIN-LINU-190924/3305
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix a deadlock problem when config TC during resetting When config TC during the reset process, may cause a deadlock, the flow is as below: pf reset start | ▼	https://git.kernel.org/stable/c/195918217448a6bb7f929d6a2ffffce9f1ece1cc, https://git.kernel.org/stable/c/67492d4d105c0a6321b00c393eec96b9a7a97a16, https://git.kernel.org/stable/c/6ae2b7d63cd056f363045eb65409143e16f23ae8	O-LIN-LINU-190924/3306

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
					

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
			UP: napi_enable()(skip) ..... | | ▼ ▼ ..... napi_disable() In reset process, the driver will DOWN the port and then UINIT, in this case, the setup tc process will UP the port before UINIT, so cause the problem. Adds a DOWN process in UINIT to fix it. **CVE ID: CVE-2024-44995**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: xhci: Fix Panther point NULL pointer deref at full-speed re-enumeration re-enumerating full-speed devices after a failed address device command	https://git.kernel.org/stable/c/0f0654318e25b2c185e245ba4a591e42fabb5e59, https://git.kernel.org/stable/c/365ef7c4277fdd781a695c3553fa157d622d805d, https://git.kernel.org/stable/c/5ad898ae82412f8a689d59829804bff2999dd0ea	O-LIN-LINU-190924/3307

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
			can trigger a NULL pointer dereference. Full-speed devices may need to reconfigure the endpoint 0 Max Packet Size value during enumeration. Usb core calls usb_ep0_reinit() in this case, which ends up calling xhci_configure_endpoint(). On Panther point xHC the xhci_configure_endpoint() function will additionally check and reserve bandwidth in software. Other hosts do this in hardware If xHC address device command fails then a new xhci_virt_device structure is allocated as part of re-enabling the slot, but the bandwidth table		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pointers are not set up properly here. This triggers the NULL pointer dereference the next time usb_ep0_reinit() is called and xhci_configure_endpoint() tries to check and reserve bandwidth [46710.713538] usb 3-1: new full-speed USB device number 5 using xhci_hcd [46710.713699] usb 3-1: Device not responding to setup address. [46710.917684] usb 3-1: Device not responding to setup address. [46711.125536] usb 3-1: device not accepting address 5, error -71 [46711.125594] BUG: kernel NULL pointer dereference, address: 0000000000000008 [46711.125600] #PF: supervisor		

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
			read access in kernel mode [46711.125603] #PF: error_code(0x0000) - not-present page [46711.125606] PGD 0 P4D 0 [46711.125610] Oops: Oops: 0000 [#1] PREEMPT SMP PTI [46711.125615] CPU: 1 PID: 25760 Comm: kworker/1:2 Not tainted 6.10.3_2 #1 [46711.125620] Hardware name: Gigabyte Technology Co., Ltd. [46711.125623] Workqueue: usb_hub_wq hub_event [usbcore] [46711.125668] RIP: 0010:xhci_reserve_bandwidth (drivers/usb/host/xhci.c Fix this by making sure bandwidth table pointers are set up correctly after a failed address device command, and		

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
			additionally by avoiding checking for bandwidth in cases like this where no actual endpoints are added or removed, i.e. only context for default control endpoint 0 is evaluated. **CVE ID: CVE-2024-45006**		
Use After Free	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netem: fix return value if duplicate enqueue fails There is a bug in netem_enqueue() introduced by commit 5845f706388a ("net: netem: fix skb length BUG_ON in __skb_to_sgvec") that can lead to a use-after-free. This commit made netem_enqueue() always return NET_XMIT_SUCCESS	https://git.kernel.org/stable/c/0486d31dd8198e22b63a4730244b38fffce6d469, https://git.kernel.org/stable/c/52d99a69f3d556c6426048c9d481b912205919d8, https://git.kernel.org/stable/c/577d6c0619467fe90f7e8e57e45cb5bd9d36014	O-LIN-LINU-190924/3308

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
			when a packet is duplicated, which can cause the parent qdisc's q.qlen to be mistakenly incremented. When this happens qlen_notify() may be skipped on the parent during destruction, leaving a dangling pointer for some classful qdiscs like DRR. There are two ways for the bug happen: - If the duplicated packet is dropped by rootq->enqueue() and then the original packet is also dropped. - If rootq->enqueue() sends the duplicated packet to a different qdisc and the original packet is dropped. In both cases NET_XMIT_SUCCESS is returned even though no packets		

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
			are enqueued at the netem qdisc. The fix is to defer the enqueue of the duplicate packet until after the original packet has been guaranteed to return NET_XMIT_SUCCESS. **CVE ID: CVE-2024-45016**		
Improper Initialization	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: initialise extack before use Fix missing initialisation of extack in flow offload. **CVE ID: CVE-2024-45018**	https://git.kernel.org/stable/c/119be227bc04f5035efa64cb823b8a5ca5e2d1c1, https://git.kernel.org/stable/c/356beb911b63a8cff34cb57f755c2a2d2ee9dec7, https://git.kernel.org/stable/c/7eafeec6be68ebd6140a830ce9ae68ad5b67ec78	O-LIN-LINU-190924/3309
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: memcg_write_event_control(): fix a user-triggerable oops	https://git.kernel.org/stable/c/046667c4d3196938e992fba0dfcde570aa85cd0e, https://git.kernel.org/stable/c/0fbe2a72e853a1052abe9bc2b7	O-LIN-LINU-190924/3310

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
			we are *not* guaranteed that anything past the terminating NUL is mapped (let alone initialized with anything sane). **CVE ID: CVE-2024-45021**	df8ddb102da227, https://git.kernel.org/stable/c/1b37ec85ad95b612307627758c6018cd9d92cca8	
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fix bitmap corruption on close_range() with CLOSE_RANGE_UNSHARE copy_fd_bitmaps(new, old, count) is expected to copy the first count/BITS_PER_LONG bits from old->full_fds_bits[] and fill the rest with zeroes. What it does is copying enough words (BITS_TO_LONGS(count/BITS_PER_LONG)), then memsets the rest.	https://git.kernel.org/stable/c/5053581fe5dfb09b58c65dd8462bf5dea71f41ff, https://git.kernel.org/stable/c/8cad3b2b3ab81ca55f37405ffd1315bcc2948058, https://git.kernel.org/stable/c/9a2fa1472083580b6c66bdaf291f591e1170123a	O-LIN-LINU-190924/3311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			That works fine, *if* all bits past the cutoff point are clear. Otherwise we are risking garbage from the last word we'd copied. For most of the callers that is true - expand_fdtable() has count equal to old->max_fds, so there's no open descriptors past count, let alone fully occupied words in ->open_fds[], which is what bits in ->full_fds_bits[] correspond to. The other caller (dup_fd()) passes sane_fdtable_size(old_fdt, max_fds), which is the smallest multiple of BITS_PER_LONG that covers all opened descriptors below max_fds. In the common case (copying on fork()) max_fds is ~0U, so all opened		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			descriptors will be below it and we are fine, by the same reasons why the call in expand_fdtable() is safe. Unfortunately, there is a case where max_fds is less than that and where we might, indeed, end up with junk in ->full_fds_bits[] - close_range(from, to, CLOSE_RANGE_UNSHARE) with * descriptor table being currently shared * 'to' being above the current capacity of descriptor table * 'from' being just under some chunk of opened descriptors. In that case we end up with observably wrong behaviour - e.g. spawn a child with CLONE_FILES, get		

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
			all descriptors in range 0..127 open, then close_range(64, ~0U, CLOSE_RANGE_UNSHARE) and watch dup(0) ending up with descriptor #128, despite #64 being observably not open. The minimally invasive fix would be to deal with that in dup_fd(). If this proves to add measurable overhead, we can go that way, but let's try to fix copy_fd_bitmaps() first. * new helper: bitmap_copy_and_expand(to, from, bits_to_copy, size). * make copy_fd_bitmaps() take the bitmap size in words, rather than bits; it's 'count' argument is always a multiple of BITS_PER_LONG, so we are not losing any information,		

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
			and that way we can use the same helper for all three bitmaps - compiler will see that count is a multiple of BITS_PER_LONG for the large ones, so it'll generate plain memcpy()+memset(). Reproducer added to tools/testing/selftests/core/close_range_test.c **CVE ID: CVE-2024-45025**		
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mmc: mmc_test: Fix NULL dereference on allocation failure If the "test->highmem = alloc_pages()" allocation fails then calling __free_pages(test->highmem) will result in a NULL dereference. Also	https://git.kernel.org/stable/c/2b507b03991f44dfb202fc2a82c9874d1b1f0c06, https://git.kernel.org/stable/c/3b4e76ceae5b5a46c968bd952f551ce173809f63, https://git.kernel.org/stable/c/9b9ba386d7bfdbc38445932c90fa9444c0524bea	O-LIN-LINU-190924/3312

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
			change the error code to -ENOMEM instead of returning success. **CVE ID: CVE-2024-45028**		
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: gtp: fix a potential NULL pointer dereference When sockfd_lookup() fails, gtp_encap_enable_socket() returns a NULL pointer, but its callers only check for error pointers thus miss the NULL pointer case. Fix it by returning an error pointer with the error code carried from sockfd_lookup(). (I found this bug during code inspection.) **CVE ID: CVE-2024-46677**	https://git.kernel.org/stable/c/28c67f0f84f889fe9f4cbda8354132b20dc9212d, https://git.kernel.org/stable/c/4643b91691e969b1b9ad54bf552d7a990cfa3b87, https://git.kernel.org/stable/c/612edd35f2a3910ab1f61c1f2338889d4ba99fa2	O-LIN-LINU-190924/3313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: pinctrl: single: fix potential NULL dereference in pcs_get_function() pinmux_generic_get_function() can return NULL and the pointer 'function' was dereferenced without checking against NULL. Add checking of pointer 'function' in pcs_get_function(). Found by code review. **CVE ID: CVE-2024-46685**	https://git.kernel.org/stable/c/0a2bab5ed161318f57134716acba0a30f3af191, https://git.kernel.org/stable/c/1c38a62f15e595346a1106025722869e87ffe044, https://git.kernel.org/stable/c/292151af6add3e5ab11b2e9916cffa5f52859a1f	O-LIN-LINU-190924/3314
Affected Version(s): From (including) 5.13 Up to (excluding) 5.15.166					
Use of Uninitialized Resource	04-Sep-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: validate vlan header Ensure there is sufficient room to	https://git.kernel.org/stable/c/0279c35d242d037abeb73d60d06a6d1bb7f672d9, https://git.kernel.org/stable/c/043a18bb6cf16adaa2f8642acfde6e8956a9caaa, https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access the protocol field of the VLAN header, validate it once before the flowtable lookup. ========== ========== ========== ======== BUG: KMSAN: uninit-value in nf_flow_offload_inet_hook+0x45a/0x5f0 net/netfilter/nf_flow_table_inet.c:32 nf_flow_offload_inet_hook+0x45a/0x5f0 net/netfilter/nf_flow_table_inet.c:32 nf_hook_entry_hookfn include/linux/netfilter.h:154 [inline] nf_hook_slow+0xf4/0x400 net/netfilter/core.c:626 nf_hook_ingress include/linux/netfilter_netdev.h:34 [inline] nf_ingress net/core/dev.c:5440 [inline]	6ea14ccb60c8ab829349979b22b58a941ec4a3ee	

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
			CVE ID: CVE-2024-44983		
Affected Version(s): From (including) 5.13 Up to (excluding) 6.1.108					
N/A	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: only mark 'subflow' endp as available Adding the following warning ... WARN_ON_ONCE(msk->pm.local_addr_used == 0) ... before decrementing the local_addr_used counter helped to find a bug when running the "remove single address" subtest from the mptcp_join.sh selftests. Removing a 'signal' endpoint will trigger the removal of all subflows	https://git.kernel.org/stable/c/322ea3778965da72862cca2a0c50253aacf65fe6, https://git.kernel.org/stable/c/43cf912b0b0fc7b4fd12cbc735d1f5afb8e1322d, https://git.kernel.org/stable/c/7fdc870d08960961408a44c569f20f50940e7d4f	O-LIN-LINU-190924/3316

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
			linked to this endpoint via mptcp_pm_nl_rm_addr_or_subflow() with rm_type == MPTCP_MIB_RMSUBFLOW. This will decrement the local_addr_used counter, which is wrong in this case because this counter is linked to 'subflow' endpoints, and here it is a 'signal' endpoint that is being removed. Now, the counter is decremented, only if the ID is being used outside of mptcp_pm_nl_rm_addr_or_subflow(), only for 'subflow' endpoints, and if the ID is not 0 -- local_addr_used is not taking into account these ones. This marking of the ID as being available, and the decrement is done no matter if a subflow using this		

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
			ID is currently available, because the subflow could have been closed before. **CVE ID: CVE-2024-45010**		
Affected Version(s): From (including) 5.14 Up to (excluding) 5.15.166					
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: ipv6: fix possible UAF in ip6_finish_output2() If skb_expand_head() returns NULL, skb has been freed and associated dst/idev could also have been freed. We need to hold rcu_read_lock() to make sure the dst and associated idev are alive. **CVE ID: CVE-2024-44986**	https://git.kernel.org/stable/c/3574d28caf9a09756ae87ad1ea096c6f47b6101e, https://git.kernel.org/stable/c/56efc253196751ece1fc535a5b582be127b0578a, https://git.kernel.org/stable/c/6ab6bf731354a6fdbaa617d1ec194960db61cf3b	O-LIN-LINU-190924/3317
N/A	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/1371d32b95972d39c1e6e4bae8b6d0df1b5737	O-LIN-LINU-190924/3318

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
			char: xillybus: Check USB endpoints when probing device Ensure, as the driver probes the device, that all endpoints that the driver may attempt to access exist and are of the correct type. All XillyUSB devices must have a Bulk IN and Bulk OUT endpoint at address 1. This is verified in xillyusb_setup_base_eps(). On top of that, a XillyUSB device may have additional Bulk OUT endpoints. The information about these endpoints' addresses is deduced from a data structure (the IDT) that the driver fetches from the device while probing it. These endpoints	31, https://git.kernel.org/stable/c/2374bf7558de915edc6ec8cb10ec3291dfab9594, https://git.kernel.org/stable/c/25ee8b2908200fc862c0434e5ad483817d50ceda	

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
			are checked in setup_channels(). A XillyUSB device never has more than one IN endpoint, as all data towards the host is multiplexed in this single Bulk IN endpoint. This is why setup_channels() only checks OUT endpoints. **CVE ID: CVE-2024-45011**		
Affected Version(s): From (including) 5.15 Up to (excluding) 5.15.166					
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent possible UAF in ip6_xmit() If skb_expand_head() returns NULL, skb has been freed and the associated dst/idev could also have been freed. We must use rcu_read_lock() to prevent a possible UAF.	https://git.kernel.org/stable/c/124b428fe28064c809e4237b0b38e97200a8a4a8, https://git.kernel.org/stable/c/2d5ff7e339d04622d8282661df36151906d0e1c7, https://git.kernel.org/stable/c/38a21c026ed2cc7232414cb166efc1923f34af17	O-LIN-LINU-190924/3319

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
			CVE ID: CVE-2024-44985		
Affected Version(s): From (including) 5.15.162 Up to (excluding) 5.15.165					
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: driver core: Fix uevent_show() vs driver detach race uevent_show() wants to de-reference dev->driver->name. There is no clean way for a device attribute to de-reference dev->driver unless that attribute is defined via (struct device_driver).dev_groups. Instead, the anti-pattern of taking the device_lock() in the attribute handler risks deadlocks with code paths that remove device attributes while holding the lock. This deadlock is typically invisible	https://git.kernel.org/stable/c/15fffc6a5624b13b428bb1c6e9088e32a55eb82c, https://git.kernel.org/stable/c/49ea4e0d862632d51667da5e7a9c88a560e9c5a1, https://git.kernel.org/stable/c/4a7c2a8387524942171037e70b80e969c3b5c05b	O-LIN-LINU-190924/3320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to lockdep given the device_lock() is marked lockdep_set_novalidate_class(), but some subsystems allocate a local lockdep key for @dev->mutex to reveal reports of the form: ========== ========== ========== ========= WARNING: possible circular locking dependency detected 6.10.0-rc7+ #275 Tainted: G OE N --- --- --- modprobe/2374 is trying to acquire lock: ffff8c2270070de0 (kn->active#6){++++}-{0:0}, at: __kernfs_remove+0xde/0x220 but task is already holding lock:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffff8c22016e88f8 (&cxl_root_key){+.+.}-{3:3}, at: device_release_driver_internal+0x39/0x210 which lock already depends on the new lock. the existing dependency chain (in reverse order) is: -> #1 (&cxl_root_key){+.+.}-{3:3}: __mutex_lock+0x99/0xc30 uevent_show+0xac/0x130 dev_attr_show+0x18/0x40 sysfs_kf_seq_show+0xac/0xf0 seq_read_iter+0x110/0x450 vfs_read+0x25b/0x340		

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
			ksys_read+0x67/0xf0 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e -> #0 (kn->active#6){++++}-{0:0}: __lock_acquire+0x121a/0x1fa0 lock_acquire+0xd6/0x2e0 kernfs_drain+0x1e9/0x200 __kernfs_remove+0xde/0x220 kernfs_remove_by_name_ns+0x5e/0xa0 device_del+0x168/0x410 device_unregister+0x13/0x60 devres_release_all+0xb8/0x110		

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
			device_unbind_cleanup+0xe/0x70 device_release_driver_internal+0x1c7/0x210 driver_detach+0x47/0x90 bus_remove_driver+0x6c/0xf0 cxl_acpi_exit+0xc/0x11 [cxl_acpi] __do_sys_delete_module.isra.0+0x181/0x260 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e The observation though is that driver objects are typically much longer lived than device objects. It is reasonable to perform lockless de-reference of a @driver pointer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			even if it is racing detach from a device. Given the infrequency of driver unregistration, use synchronize_rcu() in module_remove_driver() to close any potential races. It is potentially overkill to suffer synchronize_rcu() just to handle the rare module removal racing uevent_show() event. Thanks to Tetsuo Handa for the debug analysis of the syzbot report [1]. **CVE ID: CVE-2024-44952**		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.105					
Missing Release of Memory after Effective Lifetime	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: dsa: bcm_sf2: Fix a possible memory leak in bcm_sf2_mdio_register()	https://git.kernel.org/stable/c/7feef10768ea71d468d9bbc1e0d14c461876768c, https://git.kernel.org/stable/c/a7d2808d67570e6acae45c2a96e0d59986888	O-LIN-LINU-190924/3321

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
			bcm_sf2_mdio_register() calls of_phy_find_device() and then phy_device_remove() in a loop to remove existing PHY devices. of_phy_find_device() eventually calls bus_find_device(), which calls get_device() on the returned struct device * to increment the refcount. The current implementation does not decrement the refcount, which causes memory leak. This commit adds the missing phy_device_free() call to decrement the refcount via put_device() to balance the refcount. **CVE ID: CVE-2024-44971**	e4c, https://git.kernel.org/stable/c/b7b8d9f5e679af60c94251fd6728dde34be69a71	
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.107					
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following	https://git.kernel.org/stable/c/124b428fe2806	O-LIN-LINU-190924/3322

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
			vulnerability has been resolved: ipv6: prevent possible UAF in ip6_xmit() If skb_expand_head() returns NULL, skb has been freed and the associated dst/idev could also have been freed. We must use rcu_read_lock() to prevent a possible UAF. **CVE ID: CVE-2024-44985**	4c809e4237b0b38e97200a8a4a8, https://git.kernel.org/stable/c/2d5ff7e339d04622d8282661df36151906d0e1c7, https://git.kernel.org/stable/c/38a21c026ed2cc7232414cb166efc1923f34af17	
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: ipv6: fix possible UAF in ip6_finish_output2() If skb_expand_head() returns NULL, skb has been freed and associated dst/idev could also have been freed.	https://git.kernel.org/stable/c/3574d28caf9a09756ae87ad1ea096c6f47b6101e, https://git.kernel.org/stable/c/56efc253196751ece1fc535a5b582be127b0578a, https://git.kernel.org/stable/c/6ab6bf731354a6fdbaa617d1ec194960db61cf3b	O-LIN-LINU-190924/3323

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
			We need to hold rcu_read_lock() to make sure the dst and associated idev are alive. **CVE ID: CVE-2024-44986**		
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent UAF in ip6_send_skb() syzbot reported an UAF in ip6_send_skb() [1] After ip6_local_out() has returned, we no longer can safely dereference rt, unless we hold rcu_read_lock(). A similar issue has been fixed in commit a688caa34beb ("ipv6: take rcu lock in rawv6_send_hdrinc()") Another potential issue in	https://git.kernel.org/stable/c/24e93695b1239fbe4c31e224372be77f82dab69a, https://git.kernel.org/stable/c/571567e0277008459750f0728f246086b2659429, https://git.kernel.org/stable/c/9a3e55afa95ed4ac9eda112d4f918af645d72f25	O-LIN-LINU-190924/3324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ip6_finish_output2() is handled in a separate patch. [1] BUG: KASAN: slab-use-after-free in ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 Read of size 8 at addr ffff88806dde4858 by task syz.1.380/6530 CPU: 1 UID: 0 PID: 6530 Comm: syz.1.380 Not tainted 6.11.0-rc3-syzkaller-00306-gdf6cbc62cc9b #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/06/2024 Call Trace: <TASK> __dump_stack lib/dump_stack.c:93 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:119		

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
			print_address_description mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x143/0x180 mm/kasan/report.c:601 ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 rawv6_push_pending_frames+0x75c/0x9e0 net/ipv6/raw.c:588 rawv6_sendmsg+0x19c7/0x23c0 net/ipv6/raw.c:926 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 sock_write_iter+0x		

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
			2dd/0x400 net/socket.c:1160 do_iter_readv_writev+0x60a/0x890 vfs_writev+0x37c/0xbb0 fs/read_write.c:971 do_writev+0x1b1/0x350 fs/read_write.c:1018 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f936bf79e79 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 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 a8 ff ff ff f7 d8 64 89 01 48		

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
			RSP: 002b:00007f936cd7f038 EFLAGS: 00000246 ORIG_RAX: 0000000000000014 RAX: ffffffffffffffda RBX: 00007f936c115f80 RCX: 00007f936bf79e79 RDX: 0000000000000001 RSI: 0000000020000040 RDI: 0000000000000004 RBP: 00007f936bfe7916 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000000 R14: 00007f936c115f80 R15: 00007fff2860a7a8 </TASK>		

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
			Allocated by task 6530: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 unpoison_slab_object mm/kasan/common.c:312 [inline] __kasan_slab_alloc+0x66/0x80 mm/kasan/common.c:338 kasan_slab_alloc include/linux/kasan.h:201 [inline] slab_post_alloc_hook mm/slub.c:3988 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_noprof+0x135/0x2a0 mm/slub.c:4044 dst_alloc+0x12b/0x190 net/core/dst.c:89 ip6_blackhole_route+0x59/0x340		

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
			net/ipv6/route.c:2670 make_blackhole net/xfrm/xfrm_policy.c:3120 [inline] xfrm_lookup_route+0xd1/0x1c0 net/xfrm/xfrm_policy.c:3313 ip6_dst_lookup_flow+0x13e/0x180 net/ipv6/ip6_output.c:1257 rawv6_sendmsg+0x1283/0x23c0 net/ipv6/raw.c:898 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 ___sys_sendmsg+0x525/0x7d0 net/socket.c:2597 __sys_sendmsg net/socket.c:2651 [inline] __sys_sendmsg+0x2b0/0x3a0 net/socket.c:2680		

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
			do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 45: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 kasan_save_free_info+0x40/0x50 mm/kasan/generic.c:579 poison_slab_object+0xe0/0x150 mm/kasan/common.c:240 __kasan_slab_free+0x37/0x60 mm/kasan/common.c:256 kasan_slab_free include/linux/kasan.h:184 [inline]		

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
			slab_free_hook mm/slub.c:2252 [inline] slab_free mm/slub.c:4473 [inline] kmem_cache_free+0x145/0x350 mm/slub.c:4548 dst_destroy+0x2ac/0x460 net/core/dst.c:124 rcu_do_batch kernel/rcu/tree.c:2569 [inline] rcu_core+0xafd/0x1830 kernel/rcu/tree. ---truncated--- **CVE ID: CVE-2024-44987**		
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: atm: idt77252: prevent use after free in dequeue_rx() We can't dereference "skb" after calling vcc->push() because the skb	https://git.kernel.org/stable/c/09e086a5f72ea27c758b3f3b419a69000c32adc1, https://git.kernel.org/stable/c/1cece837e387c039225f19028df255df87a97c0d, https://git.kernel.org/stable/c/24cf390a5426aac9255205e953	O-LIN-LINU-190924/3325

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
			is released. **CVE ID: CVE-2024-44998**	3cdd7b4235d518	
Out-of-bounds Write	11-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: s390/dasd: fix error recovery leading to data corruption on ESE devices Extent Space Efficient (ESE) or thin provisioned volumes need to be formatted on demand during usual IO processing. The dasd_ese_needs_format function checks for error codes that signal the non existence of a proper track format. The check for incorrect length is to imprecise since other error cases leading to transport of insufficient data	https://git.kernel.org/stable/c/0a228896a1b3654cd461ff654f6a64e97a9c3246, https://git.kernel.org/stable/c/19f60a55b2fda49bc4f6134a5f6356ef62ee69d8, https://git.kernel.org/stable/c/5d4a304338daf83ace2887aaacafd66fe99ed5cc	O-LIN-LINU-190924/3326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			also have this flag set. This might lead to data corruption in certain error cases for example during a storage server warmstart. Fix by removing the check for incorrect length and replacing by explicitly checking for invalid track format in transport mode. Also remove the check for file protected since this is not a valid ESE handling case. **CVE ID: CVE-2024-45026**		
Use of Uninitialized Resource	04-Sep-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: validate vlan header Ensure there is sufficient room to access the protocol field of the	https://git.kernel.org/stable/c/0279c35d242d037abeb73d60d06a6d1bb7f672d9, https://git.kernel.org/stable/c/043a18bb6cf16adaa2f8642acfde6e8956a9caaa, https://git.kernel.org/stable/c/6ea14ccb60c8ab829349979b2	O-LIN-LINU-190924/3327

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
			VLAN header, validate it once before the flowtable lookup. ========== ========== ========== ======== BUG: KMSAN: uninit-value in nf_flow_offload_inet_hook+0x45a/0x5f0 net/netfilter/nf_flow_table_inet.c:32 nf_flow_offload_inet_hook+0x45a/0x5f0 net/netfilter/nf_flow_table_inet.c:32 nf_hook_entry_hookfn include/linux/netfilter.h:154 [inline] nf_hook_slow+0xf4/0x400 net/netfilter/core.c:626 nf_hook_ingress include/linux/netfilter_netdev.h:34 [inline] nf_ingress net/core/dev.c:5440 [inline] **CVE ID: CVE-2024-44983**	2b58a941ec4a3ee	

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
Use of Uninitialized Resource	04-Sep-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: gtp: pull network headers in gtp_dev_xmit() syzbot/KMSAN reported use of uninit-value in get_dev_xmit() [1] We must make sure the IPv4 or Ipv6 header is pulled in skb->head before accessing fields in them. Use pskb_inet_may_pull() to fix this issue. [1] BUG: KMSAN: uninit-value in ipv6_pdp_find drivers/net/gtp.c:220 [inline] BUG: KMSAN: uninit-value in gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] BUG: KMSAN: uninit-value in gtp_dev_xmit+0x14	https://git.kernel.org/stable/c/137d565ab89ce3584503b443bc9e00d44f482593, https://git.kernel.org/stable/c/1f6b62392453d8f36685d19b761307a8c5617ac1, https://git.kernel.org/stable/c/34ba4f29f3d9eb52dee37512059efb2afd7e966f	O-LIN-LINU-190924/3328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			24/0x2540 drivers/net/gtp.c:1281 ipv6_pdp_find drivers/net/gtp.c:220 [inline] gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281 __netdev_start_xmit include/linux/netdevice.h:4913 [inline] netdev_start_xmit include/linux/netdevice.h:4922 [inline] xmit_one net/core/dev.c:3580 [inline] dev_hard_start_xmit+0x247/0xa20 net/core/dev.c:3596 __dev_queue_xmit+0x358c/0x5610 net/core/dev.c:4423 dev_queue_xmit include/linux/netdevice.h:3105 [inline]		

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
			packet_xmit+0x9c/0x6c0 net/packet/af_packet.c:276 packet_snd net/packet/af_packet.c:3145 [inline] packet_sendmsg+0x90e3/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45		

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
			do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3994 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_node_noprof+0x6bf/0xb80 mm/slub.c:4080 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:583 __alloc_skb+0x363/0x7b0 net/core/skbuff.c:674 alloc_skb include/linux/skbuff.h:1320 [inline]		

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
			alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6526 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2815 packet_alloc_skb net/packet/af_packet.c:2994 [inline] packet_snd net/packet/af_packet.c:3088 [inline] packet_sendmsg+0x749c/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+		

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
			0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f CPU: 0 UID: 0 PID: 7115 Comm: syz.1.515 Not tainted 6.11.0-rc1-syzkaller-00043-g94ede2a3e913 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 **CVE ID: CVE-2024-44999**		
Improper Initialization	02-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/18a067240817bee8a9360539af5d79a4bf5398	O-LIN-LINU-190924/3329

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
			fuse: Initialize beyond-EOF page contents before setting uptodate fuse_notify_store(), unlike fuse_do_readpage(), does not enable page zeroing (because it can be used to change partial page contents). So fuse_notify_store() must be more careful to fully initialize page contents (including parts of the page that are beyond end-of-file) before marking the page uptodate. The current code can leave beyond-EOF page contents uninitialized, which makes these uninitialized page contents visible to userspace via mmap(). This is an information leak,	a5, https://git.kernel.org/stable/c/33168db352c7b56ae18aa55c2cae1a1c5905d30e, https://git.kernel.org/stable/c/3c0da3d163eb32f1f91891efaade027fa9b245b9	

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
			but only affects systems which do not enable init-on-alloc (via CONFIG_INIT_ON_ALLOC_DEFAULT_ON=y or the corresponding kernel command line parameter). **CVE ID: CVE-2024-44947**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bonding: fix xfrm real_dev null pointer dereference We shouldn't set real_dev to NULL because packets can be in transit and xfrm might call xdo_dev_offload_ok() in parallel. All callbacks assume real_dev is set. Example trace: kernel: BUG: unable to handle page fault for address:	https://git.kernel.org/stable/c/21816b696c172c19d53a30d45ee005cce246ed21, https://git.kernel.org/stable/c/2f72c6a66bcd7e0187ec085237fee5db27145294, https://git.kernel.org/stable/c/4582d4ff413a07d4ed8a4823c652dc5207760548	O-LIN-LINU-190924/3330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000001030 kernel: bond0: (slave eni0np1): making interface the new active one kernel: #PF: supervisor write access in kernel mode kernel: #PF: error_code(0x0002) - not-present page kernel: PGD 0 P4D 0 kernel: Oops: 0002 [#1] PREEMPT SMP kernel: CPU: 4 PID: 2237 Comm: ping Not tainted 6.7.7+ #12 kernel: Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 kernel: RIP: 0010:nsim_ipsec_offload_ok+0xc/0x20 [netdevsim] kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: Code: e0 0f 0b 48 83 7f 38 00 74 de 0f 0b 48 8b 47 08 48 8b 37 48 8b 78 40 e9 b2 e5		

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
			9a d7 66 90 0f 1f 44 00 00 48 8b 86 80 02 00 00 <83> 80 30 10 00 00 01 b8 01 00 00 00 c3 0f 1f 80 00 00 00 00 0f 1f kernel: bond0: (slave eni0np1): making interface the new active one kernel: RSP: 0018:ffffabde8155 3b98 EFLAGS: 00010246 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_ all: failed to add SA kernel: kernel: RAX: 0000000000000000 RBX: ffff9eb404e74900 RCX: ffff9eb403d97c60 kernel: RDX: ffffffffc090de10 RSI: ffff9eb404e74900 RDI: ffff9eb3c5de9e00 kernel: RBP: ffff9eb3c0a42000 R08: 0000000000000010 R09: 0000000000000014 kernel: R10: 7974203030303030 R11:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3030303030303030 R12: 0000000000000000 kernel: R13: ffff9eb3c5de9e00 R14: ffffabde81553cc8 R15: ffff9eb404c53000 kernel: FS: 00007f2a77a3ad00(0000) GS:ffff9eb43bd00000(0000) knlGS:0000000000000000 kernel: CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 kernel: CR2: 0000000000001030 CR3: 00000001122ab000 CR4: 0000000000350ef0 kernel: bond0: (slave eni0np1): making interface the new active one kernel: Call Trace: kernel: <TASK> kernel: ? __die+0x1f/0x60 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA		

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
			kernel: ? page_fault_oops+0x142/0x4c0 kernel: ? do_user_addr_fault+0x65/0x670 kernel: ? kvm_read_and_reset_apf_flags+0x3b/0x50 kernel: bond0: (slave eni0np1): making interface the new active one kernel: ? exc_page_fault+0x7b/0x180 kernel: ? asm_exc_page_fault+0x22/0x30 kernel: ? nsim_bpf_uninit+0x50/0x50 [netdevsim] kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ? nsim_ipsec_offload_ok+0xc/0x20 [netdevsim] kernel: bond0: (slave eni0np1): making interface the new active one kernel: bond_ipsec_offload_ok+0x7b/0x90 [bonding]		

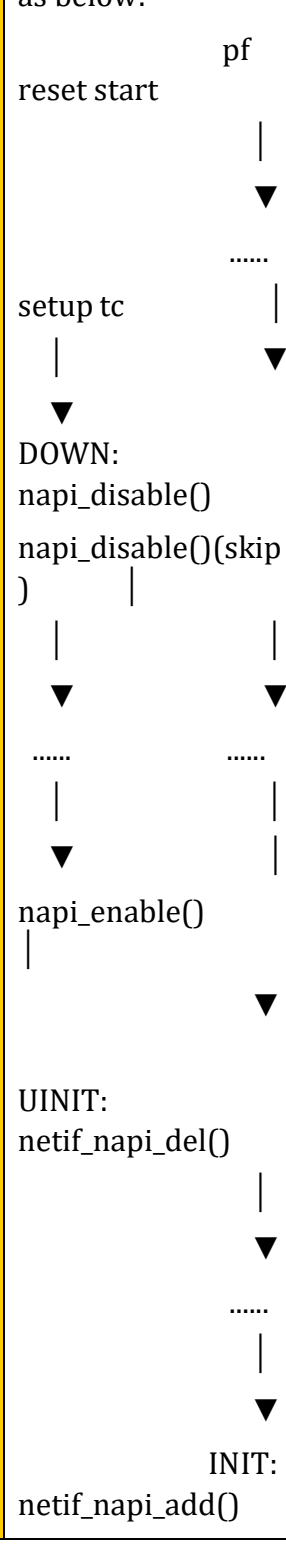
CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel: xfrm_output+0x61/0x3b0 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ip_push_pending_frames+0x56/0x80 **CVE ID: CVE-2024-44989**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bonding: fix null pointer deref in bond_ipsec_offload_ok We must check if there is an active slave before dereferencing the pointer. **CVE ID: CVE-2024-44990**	https://git.kernel.org/stable/c/0707260a18312bbcd2a5668584e3692d0a29e3f6, https://git.kernel.org/stable/c/2f5bdd68c1ce64bda6bef4d361a3de23b04ccd59, https://git.kernel.org/stable/c/32a0173600c63aadaf2103bf02f074982e8602ab	O-LIN-LINU-190924/3331
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix a deadlock problem when config TC during resetting	https://git.kernel.org/stable/c/195918217448a6bb7f929d6a2ffffce9f1ece1cc, https://git.kernel.org/stable/c/67492d4d105c0a6321b00c393eec96b9a7a97a16, https://git.kern	O-LIN-LINU-190924/3332

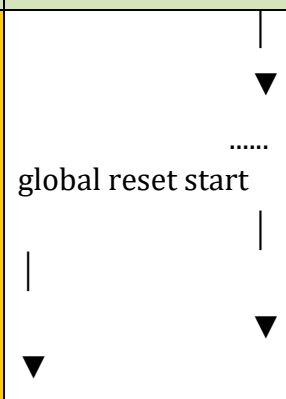
CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When config TC during the reset process, may cause a deadlock, the flow is as below: 	el.org/stable/c/6ae2b7d63cd056f363045eb65409143e16f23ae8	

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
			 In reset process, the driver will DOWN the port and then UINIT, in this case, the setup tc process will UP the port before UINIT, so cause the problem. Adds a DOWN process in UINIT to fix it. **CVE ID: CVE-2024-44995**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: xhci: Fix Panther point NULL pointer	https://git.kernel.org/stable/c/0f0654318e25b2c185e245ba4a591e42fabb5e59, https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deref at full-speed re-enumeration re-enumerating full-speed devices after a failed address device command can trigger a NULL pointer dereference. Full-speed devices may need to reconfigure the endpoint 0 Max Packet Size value during enumeration. Usb core calls usb_ep0_reinit() in this case, which ends up calling xhci_configure_endpoint(). On Panther point xHC the xhci_configure_endpoint() function will additionally check and reserve bandwidth in software. Other hosts do this in hardware	365ef7c4277fdd781a695c3553fa157d622d805d, https://git.kernel.org/stable/c/5ad898ae82412f8a689d59829804bff2999dd0ea	

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
			If xHC address device command fails then a new xhci_virt_device structure is allocated as part of re-enabling the slot, but the bandwidth table pointers are not set up properly here. This triggers the NULL pointer dereference the next time usb_ep0_reinit() is called and xhci_configure_endpoint() tries to check and reserve bandwidth [46710.713538] usb 3-1: new full-speed USB device number 5 using xhci_hcd [46710.713699] usb 3-1: Device not responding to setup address. [46710.917684] usb 3-1: Device not responding to setup address. [46711.125536] usb 3-1: device not accepting address 5, error -71		

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
			[46711.125594] BUG: kernel NULL pointer dereference, address: 0000000000000008 [46711.125600] #PF: supervisor read access in kernel mode [46711.125603] #PF: error_code(0x0000) - not-present page [46711.125606] PGD 0 P4D 0 [46711.125610] Oops: Oops: 0000 [#1] PREEMPT SMP PTI [46711.125615] CPU: 1 PID: 25760 Comm: kworker/1:2 Not tainted 6.10.3_2 #1 [46711.125620] Hardware name: Gigabyte Technology Co., Ltd. [46711.125623] Workqueue: usb_hub_wq hub_event [usbcore] [46711.125668] RIP: 0010:xhci_reserve_bandwidth		

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
			(drivers/usb/host/xhci.c Fix this by making sure bandwidth table pointers are set up correctly after a failed address device command, and additionally by avoiding checking for bandwidth in cases like this where no actual endpoints are added or removed, i.e. only context for default control endpoint 0 is evaluated. **CVE ID: CVE-2024-45006**		
N/A	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: only decrement add_addr_accepted for MPJ req Adding the following warning ...	https://git.kernel.org/stable/c/1c1f721375989579e46741f59523e39ec9b2a9bd, https://git.kernel.org/stable/c/2060f1efab370b496c4903b840844ecaff324c3c, https://git.kernel.org/stable/c/35b31f5549ede4070566b9497	O-LIN-LINU-190924/3334

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
			WARN_ON_ONCE(msk->pm.add_addr_accepted == 0) ... before decrementing the add_addr_accepted counter helped to find a bug when running the "remove single subflow" subtest from the mptcp_join.sh selftest. Removing a 'subflow' endpoint will first trigger a RM_ADDR, then the subflow closure. Before this patch, and upon the reception of the RM_ADDR, the other peer will then try to decrement this add_addr_accepted. That's not correct because the attached subflows have not been created upon the reception of an ADD_ADDR.	81e83495906b43d	

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
			A way to solve that is to decrement the counter only if the attached subflow was an MP_JOIN to a remote id that was not 0, and initiated by the host receiving the RM_ADDR. **CVE ID: CVE-2024-45009**		
N/A	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: char: xillybus: Check USB endpoints when probing device Ensure, as the driver probes the device, that all endpoints that the driver may attempt to access exist and are of the correct type. All XillyUSB devices must have a Bulk IN and Bulk OUT endpoint at address 1. This is verified in xillyusb_setup_base_eps().	https://git.kernel.org/stable/c/1371d32b95972d39c1e6e4bae8b6d0df1b573731, https://git.kernel.org/stable/c/2374bf7558de915edc6ec8cb10ec3291dfab9594, https://git.kernel.org/stable/c/25ee8b2908200fc862c0434e5ad483817d50ceda	O-LIN-LINU-190924/3335

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
			On top of that, a XillyUSB device may have additional Bulk OUT endpoints. The information about these endpoints' addresses is deduced from a data structure (the IDT) that the driver fetches from the device while probing it. These endpoints are checked in setup_channels(). A XillyUSB device never has more than one IN endpoint, as all data towards the host is multiplexed in this single Bulk IN endpoint. This is why setup_channels() only checks OUT endpoints. **CVE ID: CVE-2024-45011**		
Use After Free	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/0486d31dd8198e22b63a4730244b38fffce6d469,	O-LIN-LINU-190924/3336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			netem: fix return value if duplicate enqueue fails There is a bug in netem_enqueue() introduced by commit 5845f706388a ("net: netem: fix skb length BUG_ON in __skb_to_sgvec") that can lead to a use-after-free. This commit made netem_enqueue() always return NET_XMIT_SUCCESS when a packet is duplicated, which can cause the parent qdisc's q.qlen to be mistakenly incremented. When this happens qlen_notify() may be skipped on the parent during destruction, leaving a dangling pointer for some classful qdiscs like DRR. There are two ways for the bug happen:	https://git.kernel.org/stable/c/52d99a69f3d556c6426048c9d481b912205919d8, https://git.kernel.org/stable/c/577d6c0619467fe90f7e8e57e45cb5bd9d936014	

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
			- If the duplicated packet is dropped by rootq->enqueue() and then the original packet is also dropped. - If rootq->enqueue() sends the duplicated packet to a different qdisc and the original packet is dropped. In both cases NET_XMIT_SUCCESS is returned even though no packets are enqueued at the netem qdisc. The fix is to defer the enqueue of the duplicate packet until after the original packet has been guaranteed to return NET_XMIT_SUCCESS. **CVE ID: CVE-2024-45016**		
Improper Initialization	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/119be227bc04f5035efa64cb823b8a5ca5e2d1c	O-LIN-LINU-190924/3337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			netfilter: flowtable: initialise extack before use Fix missing initialisation of extack in flow offload. **CVE ID: CVE-2024-45018**	1, https://git.kernel.org/stable/c/356beb911b63a8cff34cb57f755c2a2d2ee9dec7, https://git.kernel.org/stable/c/7eafeec6be68ebd6140a830ce9ae68ad5b67ec78	
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: memcg_write_event_control(): fix a user-triggerable oops we are *not* guaranteed that anything past the terminating NUL is mapped (let alone initialized with anything sane). **CVE ID: CVE-2024-45021**	https://git.kernel.org/stable/c/046667c4d3196938e992fba0dfcde570aa85cd0e, https://git.kernel.org/stable/c/0fbe2a72e853a1052abe9bc2b7df8ddb102da227, https://git.kernel.org/stable/c/1b37ec85ad95b612307627758c6018cd9d92cca8	O-LIN-LINU-190924/3338
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fix bitmap corruption on close_range() with	https://git.kernel.org/stable/c/5053581fe5dfb09b58c65dd8462bf5dea71f41ff, https://git.kernel.org/stable/c/8cad3b2b3ab81	O-LIN-LINU-190924/3339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CLOSE_RANGE_UNSHARE copy_fd_bitmaps(new, old, count) is expected to copy the first count/BITS_PER_LONG bits from old->full_fds_bits[] and fill the rest with zeroes. What it does is copying enough words (BITS_TO_LONGS(count/BITS_PER_LONG)), then memsets the rest. That works fine, *if* all bits past the cutoff point are clear. Otherwise we are risking garbage from the last word we'd copied. For most of the callers that is true - expand_fdtable() has count equal to old->max_fds, so there's no open descriptors past count, let alone fully occupied words in ->open_fds[],	ca55f37405ffd1315bcc2948058, https://git.kernel.org/stable/c/9a2fa1472083580b6c66bdaf291f591e1170123a	

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
			which is what bits in ->full_fds_bits[] correspond to. The other caller (dup_fd()) passes sane_fdtable_size(old_fdt, max_fds), which is the smallest multiple of BITS_PER_LONG that covers all opened descriptors below max_fds. In the common case (copying on fork()) max_fds is ~0U, so all opened descriptors will be below it and we are fine, by the same reasons why the call in expand_fdtable() is safe. Unfortunately, there is a case where max_fds is less than that and where we might, indeed, end up with junk in ->full_fds_bits[] - close_range(from, to, CLOSE_RANGE_UNSHARE) with		

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
			* descriptor table being currently shared * 'to' being above the current capacity of descriptor table * 'from' being just under some chunk of opened descriptors. In that case we end up with observably wrong behaviour - e.g. spawn a child with CLONE_FILES, get all descriptors in range 0..127 open, then close_range(64, ~0U, CLOSE_RANGE_UNSHARE) and watch dup(0) ending up with descriptor #128, despite #64 being observably not open. The minimally invasive fix would be to deal with that in dup_fd(). If this proves to add measurable overhead, we can go that way, but		

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
			let's try to fix copy_fd_bitmaps() first. * new helper: bitmap_copy_and_expand(to, from, bits_to_copy, size). * make copy_fd_bitmaps() take the bitmap size in words, rather than bits; it's 'count' argument is always a multiple of BITS_PER_LONG, so we are not losing any information, and that way we can use the same helper for all three bitmaps - compiler will see that count is a multiple of BITS_PER_LONG for the large ones, so it'll generate plain memcpy()+memset(). Reproducer added to tools/testing/selftests/core/close_range_test.c **CVE ID: CVE-2024-45025**		

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
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mmc: mmc_test: Fix NULL dereference on allocation failure If the "test->highmem = alloc_pages()" allocation fails then calling __free_pages(test->highmem) will result in a NULL dereference. Also change the error code to -ENOMEM instead of returning success. **CVE ID: CVE-2024-45028**	https://git.kernel.org/stable/c/2b507b03991f44dfb202fc2a82c9874d1b1f0c06, https://git.kernel.org/stable/c/3b4e76ceae5b5a46c968bd952f551ce173809f63, https://git.kernel.org/stable/c/9b9ba386d7bfdbc38445932c90fa9444c0524bea	O-LIN-LINU-190924/3340
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.108					
Double Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: scsi: aacraid: Fix double-free on probe failure aac_probe_one() calls hardware-specific init	https://git.kernel.org/stable/c/4b540ec7c0045c2d01c4e479f34bbc8f147afa4c, https://git.kernel.org/stable/c/564e1986b00c5f05d75342f8407f75f0a17b94df, https://git.kernel.org/stable/c/60962c3d8e18e	O-LIN-LINU-190924/3341

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
			functions through the aac_driver_ident::init pointer, all of which eventually call down to aac_init_adapter(). If aac_init_adapter() fails after allocating memory for aac_dev::queues, it frees the memory but does not clear that member. After the hardware-specific init function returns an error, aac_probe_one() goes down an error path that frees the memory pointed to by aac_dev::queues, resulting.in a double-free. **CVE ID: CVE-2024-46673**	5d8dfa16df788974dd7f35bd87a	
Use After Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: dwc3: st: fix probed platform device ref count on probe error path	https://git.kernel.org/stable/c/060f41243ad7f6f5249fa7290dda0c01f723d12d, https://git.kernel.org/stable/c/1de989668708ce5875efc9d66	O-LIN-LINU-190924/3342

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 probe function never performs any paltform device allocation, thus error path "undo_platform_dev_alloc" is entirely bogus. It drops the reference count from the platform device being probed. If error path is triggered, this will lead to unbalanced device reference counts and premature release of device resources, thus possible use-after-free when releasing remaining devm-managed resources. **CVE ID: CVE-2024-46674**	9d227212aeb9a90, https://git.kernel.org/stable/c/4c6735299540f3c82a5033d35be76a5c42e0fb18	
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: gtp: fix a potential NULL pointer dereference When sockfd_lookup() fails,	https://git.kernel.org/stable/c/28c67f0f84f889fe9f4cbda8354132b20dc9212d, https://git.kernel.org/stable/c/4643b91691e969b1b9ad54bf552d7a990cfa3b87, https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gtp_encap_enable_socket() returns a NULL pointer, but its callers only check for error pointers thus miss the NULL pointer case. Fix it by returning an error pointer with the error code carried from sockfd_lookup(). (I found this bug during code inspection.) **CVE ID: CVE-2024-46677**	612edd35f2a3910ab1f61c1f2338889d4ba99fa2	
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: pinctrl: single: fix potential NULL dereference in pcs_get_function() pinmux_generic_get_function() can return NULL and the pointer 'function' was dereferenced without checking against NULL. Add checking of pointer	https://git.kernel.org/stable/c/0a2bab5ed161318f57134716accba0a30f3af191, https://git.kernel.org/stable/c/1c38a62f15e595346a1106025722869e87ffe044, https://git.kernel.org/stable/c/292151af6add3e5ab11b2e9916cffa5f52859a1f	O-LIN-LINU-190924/3344

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
			'function' in pcs_get_function(). Found by code review. **CVE ID: CVE-2024-46685**		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.55					
NULL Pointer Dereference	06-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: media: dvb-usb-v2: af9035: Fix null-ptr-deref in af9035_i2c_master_xfer In af9035_i2c_master_xfer, msg is controlled by user. When msg[i].buf is null and msg[i].len is zero, former checks on msg[i].buf would be passed. Malicious data finally reach af9035_i2c_master_xfer. If accessing msg[i].buf[0] without sanity check, null ptr deref would happen. We add check on msg[i].len to prevent crash.	https://git.kernel.org/stable/c/0143f282b15f7cedc0392ea10050fb6000fd16e6, https://git.kernel.org/stable/c/41b7181a40af84448a2b144fb02d8bf32b7e9a23, https://git.kernel.org/stable/c/6c01ef65de0b321b2db1ef9abf8f1d15862b937e	O-LIN-LINU-190924/3345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Similar commit: commit 0ed554fd769a ("media: dvb-usb: az6027: fix null-ptr-deref in az6027_i2c_xfer()") **CVE ID: CVE-2023-52915**		
Affected Version(s): From (including) 5.17 Up to (excluding) 6.1.107					
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fs/netfs/fscache_cookie: add missing "n_accesses" check This fixes a NULL pointer dereference bug due to a data race which looks like this: BUG: kernel NULL pointer dereference, address: 0000000000000008 #PF: supervisor read access in kernel mode	https://git.kernel.org/stable/c/0a4d41fa14b2a0efd40e350cfe8ec6a4c998ac1d, https://git.kernel.org/stable/c/b8a50877f68efdcc0be3fcc5116e00c31b90e45b, https://git.kernel.org/stable/c/dfaa39b05a6cf34a16c525a2759ee6ab26b5fef6	O-LIN-LINU-190924/3346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			#PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] SMP PTI CPU: 33 PID: 16573 Comm: kworker/u97:799 Not tainted 6.8.7-cm4all1-hp+ #43 Hardware name: HP ProLiant DL380 Gen9/ProLiant DL380 Gen9, BIOS P89 10/17/2018 Workqueue: events_unbound netfs_rreq_write_to_cache_work RIP: 0010:cachefiles_prepare_write+0x30/0xa0 Code: 57 41 56 45 89 ce 41 55 49 89 cd 41 54 49 89 d4 55 53 48 89 fb 48 83 ec 08 48 8b 47 08 48 83 7f 10 00 48 89 34 24 48 8b 68 20 <48> 8b 45 08 4c 8b 38 74 45 49 8b 7f 50 e8 4e a9 b0 ff 48 8b 73 10 RSP: 0018:ffffb4e78113bde0 EFLAGS: 00010286 RAX: ffff976126be6d10		

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
			RBX: ffff97615cdb8438 RCX: 0000000000020000 RDX: ffff97605e6c4c68 RSI: ffff97605e6c4c60 RDI: ffff97615cdb8438 RBP: 0000000000000000 R08: 0000000002783333 R09: 0000000000000001 R10: ffff97605e6c4600 R11: 0000000000000001 R12: ffff97605e6c4c68 R13: 0000000000020000 R14: 0000000000000001 R15: ffff976064fe2c00 FS: 0000000000000000(0000) GS:ffff9776dfd40000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033		

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
			CR2: 0000000000000008 CR3: 000000005942c002 CR4: 00000000001706f0 Call Trace: <TASK> ? __die+0x1f/0x70 ? page_fault_oops+0x15d/0x440 ? search_module_extables+0xe/0x40 ? fixup_exception+0x22/0x2f0 ? exc_page_fault+0x5f/0x100 ? asm_exc_page_fault+0x22/0x30 ? cachefiles_prepare_write+0x30/0xa0 netfs_rreq_write_to_cache_work+0x135/0x2e0 process_one_work+0x137/0x2c0 worker_thread+0x2e9/0x400		

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
			? __pfx_worker_thread+0x10/0x10 kthread+0xcc/0x100 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x30/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1b/0x30 </TASK> Modules linked in: CR2: 0000000000000008 ---[end trace 0000000000000000]--- This happened because fscache_cookie_state_machine() was slow and was still running while another process invoked fscache_unuse_cookie(); this led to a fscache_cookie_lru_		

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

			do_one() call, setting the FSCACHE_COOKIE_DO_LRU_DISCARD flag, which was picked up by fscache_cookie_state_machine(), withdrawing the cookie via cachefiles_withdraw_cookie(), clearing cookie->cache_priv.
			
			At the same time, yet another process invoked cachefiles_prepare_write(), which found a NULL pointer in this code line:
			
			struct cachefiles_object *object = cachefiles_cres_object(cres);
			
			The next line crashes, obviously:
			
			struct cachefiles_cache *cache = object->volume->cache;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			During cachefiles_prepare_write(), the "n_accesses" counter is non-zero (via fscache_begin_operation()). The cookie must not be withdrawn until it drops to zero. The counter is checked by fscache_cookie_state_machine() before switching to FSCACHE_COOKIE_STATE_RELINQUISHING and FSCACHE_COOKIE_STATE_WITHDRAWING (in "case FSCACHE_COOKIE_STATE_FAILED"), but not for FSCACHE_COOKIE_STATE_LRU_DISCARDING ("case FSCACHE_COOKIE_STATE_ACTIVE"). This patch adds the missing check. With a non-zero access counter, the function returns and the next		

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
			fscache_end_cookie_access() call will queue another fscache_cookie_state_machine() call to handle the still-pending FSCACHE_COOKIE_DO_LRU_DISCARD. **CVE ID: CVE-2024-45000**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: rtla/osnoise: Prevent NULL dereference in error handling If the "tool->data" allocation fails then there is no need to call osnoise_free_top() and, in fact, doing so will lead to a NULL dereference. **CVE ID: CVE-2024-45002**	https://git.kernel.org/stable/c/753f1745146e03abd17eec8eee95faffc96d743d, https://git.kernel.org/stable/c/90574d2a675947858b47008df8d07f75ea50d0d0, https://git.kernel.org/stable/c/abdb9ddaaab476e62805e36cce7b4ef8413ffd01	O-LIN-LINU-190924/3347
Improper Locking	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: i2c: tegra: Do not mark ACPI devices as irq safe	https://git.kernel.org/stable/c/14d069d92951a3e150c0a81f2ca3b93e54da913b, https://git.kernel.org/stable/c/2853e1376d81	O-LIN-LINU-190924/3348

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
			On ACPI machines, the tegra i2c module encounters an issue due to a mutex being called inside a spinlock. This leads to the following bug: BUG: sleeping function called from invalid context at kernel/locking/mutex.c:585 ... Call trace: __might_sleep __mutex_lock_common mutex_lock_nested acpi_subsys_runtime_resume rpm_resume tegra_i2c_xfer The problem arises because during __pm_runtime_resume(), the spinlock &dev->power.lock is acquired before	61b04c9ff18ba82b43f08a049905, https://git.kernel.org/stable/c/6861faf4232e4b78878f2de1ed3ee324ddae2287	

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
			rpm_resume() is called. Later, rpm_resume() invokes acpi_subsys_runtime_resume(), which relies on mutexes, triggering the error. To address this issue, devices on ACPI are now marked as not IRQ-safe, considering the dependency of acpi_subsys_runtime_resume() on mutexes. **CVE ID: CVE-2024-45029**		
Affected Version(s): From (including) 5.3 Up to (excluding) 5.4.283					
Out-of-bounds Write	11-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: s390/dasd: fix error recovery leading to data corruption on ESE devices Extent Space Efficient (ESE) or thin provisioned volumes need to be formatted on demand during	https://git.kernel.org/stable/c/0a228896a1b3654cd461ff654f6a64e97a9c3246, https://git.kernel.org/stable/c/19f60a55b2fda49bc4f6134a5f6356ef62ee69d8, https://git.kernel.org/stable/c/5d4a304338daf83ace2887aaacafd66fe99ed5cc	O-LIN-LINU-190924/3349

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
			usual IO processing. The dasd_ese_needs_format function checks for error codes that signal the non existence of a proper track format. The check for incorrect length is to imprecise since other error cases leading to transport of insufficient data also have this flag set. This might lead to data corruption in certain error cases for example during a storage server warmstart. Fix by removing the check for incorrect length and replacing by explicitly checking for invalid track format in transport mode. Also remove the check for file		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected since this is not a valid ESE handling case. **CVE ID: CVE-2024-45026**		
Affected Version(s): From (including) 5.4.279 Up to (excluding) 5.4.282					
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: driver core: Fix uevent_show() vs driver detach race uevent_show() wants to de-reference dev->driver->name. There is no clean way for a device attribute to de-reference dev->driver unless that attribute is defined via (struct device_driver).dev_groups. Instead, the anti-pattern of taking the device_lock() in the attribute handler risks deadlocks with code paths that remove device attributes while holding the lock.	https://git.kernel.org/stable/c/15fffc6a5624b13b428bb1c6e9088e32a55eb82c, https://git.kernel.org/stable/c/49ea4e0d862632d51667da5e7a9c88a560e9c5a1, https://git.kernel.org/stable/c/4a7c2a8387524942171037e70b80e969c3b5c05b	O-LIN-LINU-190924/3350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This deadlock is typically invisible to lockdep given the device_lock() is marked lockdep_set_novalidate_class(), but some subsystems allocate a local lockdep key for @dev->mutex to reveal reports of the form: ========== ========== ========== ========= WARNING: possible circular locking dependency detected 6.10.0-rc7+ #275 Tainted: G OE N --- --- --- modprobe/2374 is trying to acquire lock: ffff8c2270070de0 (kn->active#6){++++}-{0:0}, at: __kernfs_remove+0xde/0x220		

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
			but task is already holding lock: ffff8c22016e88f8 (&cxl_root_key){+.+.}-{3:3}, at: device_release_driver_internal+0x39/0x210 which lock already depends on the new lock. the existing dependency chain (in reverse order) is: -> #1 (&cxl_root_key){+.+.}-{3:3}: __mutex_lock+0x99/0xc30 uevent_show+0xac/0x130 dev_attr_show+0x18/0x40 sysfs_kf_seq_show+0xac/0xf0 seq_read_iter+0x110/0x450		

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
			vfs_read+0x25b/0x340 ksys_read+0x67/0xf0 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e -> #0 (kn->active#6){++++}-{0:0}: __lock_acquire+0x121a/0x1fa0 lock_acquire+0xd6/0x2e0 kernfs_drain+0x1e9/0x200 __kernfs_remove+0xde/0x220 kernfs_remove_by_name_ns+0x5e/0xa0 device_del+0x168/0x410 device_unregister+0x13/0x60		

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
			devres_release_all+0xb8/0x110 device_unbind_cleanup+0xe/0x70 device_release_driver_internal+0x1c7/0x210 driver_detach+0x47/0x90 bus_remove_driver+0x6c/0xf0 cxl_acpi_exit+0xc/0x11 [cxl_acpi] __do_sys_delete_module.isra.0+0x181/0x260 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e The observation though is that driver objects are typically much longer lived than device objects. It is reasonable to perform lockless		

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
			de-reference of a @driver pointer even if it is racing detach from a device. Given the infrequency of driver unregistration, use synchronize_rcu() in module_remove_driver() to close any potential races. It is potentially overkill to suffer synchronize_rcu() just to handle the rare module removal racing uevent_show() event. Thanks to Tetsuo Handa for the debug analysis of the syzbot report [1]. **CVE ID: CVE-2024-44952**		
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.197					
NULL Pointer Dereference	06-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: media: dvb-usb-v2: af9035: Fix null-ptr-deref in	https://git.kernel.org/stable/c/0143f282b15f7cedc0392ea10050fb6000fd16e6, https://git.kernel.org/stable/c/41b7181a40af8	O-LIN-LINU-190924/3351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			af9035_i2c_master_xfer In af9035_i2c_master_xfer, msg is controlled by user. When msg[i].buf is null and msg[i].len is zero, former checks on msg[i].buf would be passed. Malicious data finally reach af9035_i2c_master_xfer. If accessing msg[i].buf[0] without sanity check, null ptr deref would happen. We add check on msg[i].len to prevent crash. Similar commit: commit 0ed554fd769a ("media: dvb-usb: az6027: fix null-ptr-deref in az6027_i2c_xfer()") **CVE ID: CVE-2023-52915**	4448a2b144fb02d8bf32b7e9a23, https://git.kernel.org/stable/c/6c01ef65de0b321b2db1ef9abf8f1d15862b937e	
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.225					
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/24e93695b1239fbe4c31e224372be77f82dab6	O-LIN-LINU-190924/3352

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
			ipv6: prevent UAF in ip6_send_skb() syzbot reported an UAF in ip6_send_skb() [1] After ip6_local_out() has returned, we no longer can safely dereference rt, unless we hold rcu_read_lock(). A similar issue has been fixed in commit a688caa34beb ("ipv6: take rcu lock in rawv6_send_hdrinc()") Another potential issue in ip6_finish_output2() is handled in a separate patch. [1] BUG: KASAN: slab-use-after-free in ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964	9a, https://git.kernel.org/stable/c/571567e0277008459750f0728f246086b2659429, https://git.kernel.org/stable/c/9a3e55afa95ed4ac9eda112d4f918af645d72f25	

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
			Read of size 8 at addr ffff88806dde4858 by task syz.1.380/6530 CPU: 1 UID: 0 PID: 6530 Comm: syz.1.380 Not tainted 6.11.0-rc3-syzkaller-00306-gdf6cbc62cc9b #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/06/2024 Call Trace: <TASK> __dump_stack lib/dump_stack.c:93 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:119 print_address_description mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x14		

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
			3/0x180 mm/kasan/report.c:601 ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 rawv6_push_pending_frames+0x75c/0x9e0 net/ipv6/raw.c:588 rawv6_sendmsg+0x19c7/0x23c0 net/ipv6/raw.c:926 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 sock_write_iter+0x2dd/0x400 net/socket.c:1160 do_iter_readv_writev+0x60a/0x890 vfs_writev+0x37c/0xbb0 fs/read_write.c:971 do_writev+0x1b1/		

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
			0x350 fs/read_write.c:1018 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f936bf79e79 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 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 a8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f936cd7f038 EFLAGS: 00000246 ORIG_RAX: 0000000000000014 RAX: ffffffffffffffda RBX: 00007f936c115f80 RCX: 00007f936bf79e79		

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
			RDX: 0000000000000001 RSI: 0000000020000040 RDI: 0000000000000004 RBP: 00007f936bfe7916 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000000 R14: 00007f936c115f80 R15: 00007fff2860a7a8 </TASK> Allocated by task 6530: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 unpoison_slab_obje		

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
			ct mm/kasan/common.c:312 [inline] __kasan_slab_alloc+0x66/0x80 mm/kasan/common.c:338 kasan_slab_alloc include/linux/kasan.h:201 [inline] slab_post_alloc_hook mm/slub.c:3988 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_noprof+0x135/0x2a0 mm/slub.c:4044 dst_alloc+0x12b/0x190 net/core/dst.c:89 ip6_blackhole_route+0x59/0x340 net/ipv6/route.c:2670 make_blackhole net/xfrm/xfrm_policy.c:3120 [inline] xfrm_lookup_route+0xd1/0x1c0 net/xfrm/xfrm_policy.c:3313 ip6_dst_lookup_flo		

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
			w+0x13e/0x180 net/ipv6/ip6_output.c:1257 rawv6_sendmsg+0x1283/0x23c0 net/ipv6/raw.c:898 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 ___sys_sendmsg+0x525/0x7d0 net/socket.c:2597 ___sys_sendmsg net/socket.c:2651 [inline] __sys_sendmsg+0x2b0/0x3a0 net/socket.c:2680 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f		

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
			Freed by task 45: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 kasan_save_free_info+0x40/0x50 mm/kasan/generic.c:579 poison_slab_object+0xe0/0x150 mm/kasan/common.c:240 __kasan_slab_free+0x37/0x60 mm/kasan/common.c:256 kasan_slab_free include/linux/kasan.h:184 [inline] slab_free_hook mm/slub.c:2252 [inline] slab_free mm/slub.c:4473 [inline] kmem_cache_free+0x145/0x350 mm/slub.c:4548 dst_destroy+0x2ac		

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
			/0x460 net/core/dst.c:124 rcu_do_batch kernel/rcu/tree.c:2569 [inline] rcu_core+0xafd/0x1830 kernel/rcu/tree. ---truncated--- **CVE ID: CVE-2024-44987**		
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: atm: idt77252: prevent use after free in dequeue_rx() We can't dereference "skb" after calling vcc->push() because the skb is released. **CVE ID: CVE-2024-44998**	https://git.kernel.org/stable/c/09e086a5f72ea27c758b3f3b419a69000c32adc1, https://git.kernel.org/stable/c/1cece837e387c039225f19028df255df87a97c0d, https://git.kernel.org/stable/c/24cf390a5426aac9255205e9533cdd7b4235d518	O-LIN-LINU-190924/3353
Out-of-bounds Write	11-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: s390/dasd: fix error recovery leading to data	https://git.kernel.org/stable/c/0a228896a1b3654cd461ff654f6a64e97a9c3246, https://git.kernel.org/stable/c/19f60a55b2fda49bc4f6134a5f	O-LIN-LINU-190924/3354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corruption on ESE devices Extent Space Efficient (ESE) or thin provisioned volumes need to be formatted on demand during usual IO processing. The dasd_ese_needs_format function checks for error codes that signal the non existence of a proper track format. The check for incorrect length is to imprecise since other error cases leading to transport of insufficient data also have this flag set. This might lead to data corruption in certain error cases for example during a storage server warmstart. Fix by removing the check for incorrect	6356ef62ee69d8, https://git.kernel.org/stable/c/5d4a304338daf83ace2887aaacafd66fe99ed5cc	

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
			length and replacing by explicitly checking for invalid track format in transport mode. Also remove the check for file protected since this is not a valid ESE handling case. **CVE ID: CVE-2024-45026**		
Double Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: scsi: aacraid: Fix double-free on probe failure aac_probe_one() calls hardware-specific init functions through the aac_driver_ident::init pointer, all of which eventually call down to aac_init_adapter(). If aac_init_adapter() fails after allocating memory for aac_dev::queues,	https://git.kernel.org/stable/c/4b540ec7c0045c2d01c4e479f34bbc8f147afa4c, https://git.kernel.org/stable/c/564e1986b00c5f05d75342f8407f75f0a17b94df, https://git.kernel.org/stable/c/60962c3d8e18e5d8dfa16df788974dd7f35bd87a	O-LIN-LINU-190924/3355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it frees the memory but does not clear that member. After the hardware-specific init function returns an error, aac_probe_one() goes down an error path that frees the memory pointed to by aac_dev::queues, resulting.in a double-free. **CVE ID: CVE-2024-46673**		
Use After Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: dwc3: st: fix probed platform device ref count on probe error path The probe function never performs any paltform device allocation, thus error path "undo_platform_dev_alloc" is entirely bogus. It drops the reference count from the platform device being probed. If error path is	https://git.kernel.org/stable/c/060f41243ad7f6f5249fa7290dda0c01f723d12d, https://git.kernel.org/stable/c/1de989668708ce5875efc9d669d227212aeb9a90, https://git.kernel.org/stable/c/4c6735299540f3c82a5033d35be76a5c42e0fb18	O-LIN-LINU-190924/3356

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
			triggered, this will lead to unbalanced device reference counts and premature release of device resources, thus possible use-after-free when releasing remaining devm-managed resources. **CVE ID: CVE-2024-46674**		
Use of Uninitialized Resource	04-Sep-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: gtp: pull network headers in gtp_dev_xmit() syzbot/KMSAN reported use of uninit-value in get_dev_xmit() [1] We must make sure the IPv4 or Ipv6 header is pulled in skb->head before accessing fields in them. Use pskb_inet_may_pull() to fix this issue.	https://git.kernel.org/stable/c/137d565ab89ce3584503b443bc9e00d44f482593, https://git.kernel.org/stable/c/1f6b62392453d8f36685d19b761307a8c5617ac1, https://git.kernel.org/stable/c/34ba4f29f3d9eb52dee37512059efb2afd7e966f	O-LIN-LINU-190924/3357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[1] BUG: KMSAN: uninit-value in ipv6_pdp_find drivers/net/gtp.c:220 [inline] BUG: KMSAN: uninit-value in gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] BUG: KMSAN: uninit-value in gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281 ipv6_pdp_find drivers/net/gtp.c:220 [inline] gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281 __netdev_start_xmit include/linux/netdevice.h:4913 [inline] netdev_start_xmit include/linux/netdevice.h:4922 [inline] xmit_one net/core/dev.c:3580 [inline]		

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
			dev_hard_start_xmit+0x247/0xa20 net/core/dev.c:3596 __dev_queue_xmit+0x358c/0x5610 net/core/dev.c:4423 dev_queue_xmit include/linux/netdevice.h:3105 [inline] packet_xmit+0x9c/0x6c0 net/packet/af_packet.c:276 packet_snd net/packet/af_packet.c:3145 [inline] packet_sendmsg+0x90e3/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204		

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
			__do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3994 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_		

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
			node_noprof+0x6bf/0xb80 mm/slub.c:4080 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:583 __alloc_skb+0x363/0x7b0 net/core/skbuff.c:674 alloc_skb include/linux/skbuff.h:1320 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6526 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2815 packet_alloc_skb net/packet/af_packet.c:2994 [inline] packet_snd net/packet/af_packet.c:3088 [inline] packet_sendmsg+0x749c/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline]		

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
			__sock_sendmsg+0x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f CPU: 0 UID: 0 PID: 7115 Comm: syz.1.515 Not tainted 6.11.0-rc1-		

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
			syzkaller-00043-g94ede2a3e913 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 **CVE ID: CVE-2024-44999**		
Improper Initialization	02-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fuse: Initialize beyond-EOF page contents before setting uptodate fuse_notify_store(), unlike fuse_do_readpage(), does not enable page zeroing (because it can be used to change partial page contents). So fuse_notify_store() must be more careful to fully initialize page contents (including parts of the page that are beyond end-of-file)	https://git.kernel.org/stable/c/18a067240817bee8a9360539af5d79a4bf5398a5, https://git.kernel.org/stable/c/33168db352c7b56ae18aa55c2cae1a1c5905d30e, https://git.kernel.org/stable/c/3c0da3d163eb32f1f91891efaade027fa9b245b9	O-LIN-LINU-190924/3358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before marking the page uptodate. The current code can leave beyond-EOF page contents uninitialized, which makes these uninitialized page contents visible to userspace via mmap(). This is an information leak, but only affects systems which do not enable init-on-alloc (via CONFIG_INIT_ON_ALLOC_DEFAULT_ON=y or the corresponding kernel command line parameter). **CVE ID: CVE-2024-44947**		
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix a deadlock problem when config TC during resetting When config TC during the reset	https://git.kernel.org/stable/c/195918217448a6bb7f929d6a2ffffce9f1ece1cc, https://git.kernel.org/stable/c/67492d4d105c0a6321b00c393eec96b9a7a97a16, https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process, may cause a deadlock, the flow is as below: pf reset start | ▼ ..... setup tc | | ▼ ▼ DOWN: napi_disable() napi_disable()(skip) | | | ▼ ▼ .... | | ▼ | napi_enable() | ▼ UINIT: netif_napi_del() | ▼ ..... | ▼ INIT: netif_napi_add() |	6ae2b7d63cd056f363045eb65409143e16f23ae8	

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
			▼ ..... global reset start | | ▼ ▼ UP: napi_enable()(skip) ..... | | ▼ ▼ ..... napi_disable() In reset process, the driver will DOWN the port and then UINIT, in this case, the setup tc process will UP the port before UINIT, so cause the problem. Adds a DOWN process in UINIT to fix it. **CVE ID: CVE-2024-44995**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: xhci: Fix Panther point NULL pointer deref at full-speed re-enumeration	https://git.kernel.org/stable/c/0f0654318e25b2c185e245ba4a591e42fabb5e59, https://git.kernel.org/stable/c/365ef7c4277fdd781a695c355	O-LIN-LINU-190924/3360

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
			re-enumerating full-speed devices after a failed address device command can trigger a NULL pointer dereference. Full-speed devices may need to reconfigure the endpoint 0 Max Packet Size value during enumeration. Usb core calls usb_ep0_reinit() in this case, which ends up calling xhci_configure_endpoint(). On Panther point xHC the xhci_configure_endpoint() function will additionally check and reserve bandwidth in software. Other hosts do this in hardware If xHC address device command fails then a new	3fa157d622d805d, https://git.kernel.org/stable/c/5ad898ae82412f8a689d59829804bff2999dd0ea	

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
			xhci_virt_device structure is allocated as part of re-enabling the slot, but the bandwidth table pointers are not set up properly here. This triggers the NULL pointer dereference the next time usb_ep0_reinit() is called and xhci_configure_endpoint() tries to check and reserve bandwidth [46710.713538] usb 3-1: new full-speed USB device number 5 using xhci_hcd [46710.713699] usb 3-1: Device not responding to setup address. [46710.917684] usb 3-1: Device not responding to setup address. [46711.125536] usb 3-1: device not accepting address 5, error -71 [46711.125594] BUG: kernel NULL pointer dereference,		

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
			address: 0000000000000008 [46711.125600] #PF: supervisor read access in kernel mode [46711.125603] #PF: error_code(0x0000) - not-present page [46711.125606] PGD 0 P4D 0 [46711.125610] Oops: Oops: 0000 [#1] PREEMPT SMP PTI [46711.125615] CPU: 1 PID: 25760 Comm: kworker/1:2 Not tainted 6.10.3_2 #1 [46711.125620] Hardware name: Gigabyte Technology Co., Ltd. [46711.125623] Workqueue: usb_hub_wq hub_event [usbcore] [46711.125668] RIP: 0010:xhci_reserve_bandwidth (drivers/usb/host/xhci.c Fix this by making sure bandwidth		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			table pointers are set up correctly after a failed address device command, and additionally by avoiding checking for bandwidth in cases like this where no actual endpoints are added or removed, i.e. only context for default control endpoint 0 is evaluated. **CVE ID: CVE-2024-45006**		
Use After Free	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netem: fix return value if duplicate enqueue fails There is a bug in netem_enqueue() introduced by commit 5845f706388a ("net: netem: fix skb length BUG_ON in __skb_to_sgvec") that can lead to a use-after-free.	https://git.kernel.org/stable/c/0486d31dd8198e22b63a4730244b38fffce6d469, https://git.kernel.org/stable/c/52d99a69f3d556c6426048c9d481b912205919d8, https://git.kernel.org/stable/c/577d6c0619467fe90f7e8e57e45cb5bd9d936014	O-LIN-LINU-190924/3361

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
			This commit made netem_enqueue() always return NET_XMIT_SUCCESS when a packet is duplicated, which can cause the parent qdisc's q.qlen to be mistakenly incremented. When this happens qlen_notify() may be skipped on the parent during destruction, leaving a dangling pointer for some classful qdiscs like DRR. There are two ways for the bug happen: - If the duplicated packet is dropped by rootq->enqueue() and then the original packet is also dropped. - If rootq->enqueue() sends the duplicated packet to a different qdisc and the original packet is dropped.		

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
			In both cases NET_XMIT_SUCCESS is returned even though no packets are enqueued at the netem qdisc. The fix is to defer the enqueue of the duplicate packet until after the original packet has been guaranteed to return NET_XMIT_SUCCESS. **CVE ID: CVE-2024-45016**		
Improper Initialization	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: initialise extack before use Fix missing initialisation of extack in flow offload. **CVE ID: CVE-2024-45018**	https://git.kernel.org/stable/c/119be227bc04f5035efa64cb823b8a5ca5e2d1c1, https://git.kernel.org/stable/c/356beb911b63a8cff34cb57f755c2a2d2ee9dec7, https://git.kernel.org/stable/c/7eafeec6be68ebd6140a830ce9ae68ad5b67ec78	O-LIN-LINU-190924/3362
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/046667c4d3196938e992fba0dfcde570aa85cd0e,	O-LIN-LINU-190924/3363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memcg_write_event_control(): fix a user-triggerable oops we are *not* guaranteed that anything past the terminating NUL is mapped (let alone initialized with anything sane). **CVE ID: CVE-2024-45021**	https://git.kernel.org/stable/c/0fbe2a72e853a1052abe9bc2b7df8ddb102da227, https://git.kernel.org/stable/c/1b37ec85ad95b612307627758c6018cd9d92cca8	
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fix bitmap corruption on close_range() with CLOSE_RANGE_UNSHARE copy_fd_bitmaps(new, old, count) is expected to copy the first count/BITS_PER_LONG bits from old->full_fds_bits[] and fill the rest with zeroes. What it does is copying enough words (BITS_TO_LONGS(count/BITS_PER_LO	https://git.kernel.org/stable/c/5053581fe5dfb09b58c65dd8462bf5dea71f41ff, https://git.kernel.org/stable/c/8cad3b2b3ab81ca55f37405ffd1315bcc2948058, https://git.kernel.org/stable/c/9a2fa1472083580b6c66bdaf291f591e1170123a	O-LIN-LINU-190924/3364

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
			NG)), then memsets the rest. That works fine, *if* all bits past the cutoff point are clear. Otherwise we are risking garbage from the last word we'd copied. For most of the callers that is true - expand_fdtable() has count equal to old->max_fds, so there's no open descriptors past count, let alone fully occupied words in ->open_fds[], which is what bits in ->full_fds_bits[] correspond to. The other caller (dup_fd()) passes sane_fdtable_size(old_fdt, max_fds), which is the smallest multiple of BITS_PER_LONG that covers all opened descriptors below max_fds. In the common case (copying on		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fork()) max_fds is ~0U, so all opened descriptors will be below it and we are fine, by the same reasons why the call in expand_fdtable() is safe. Unfortunately, there is a case where max_fds is less than that and where we might, indeed, end up with junk in ->full_fds_bits[] - close_range(from, to, CLOSE_RANGE_UNSHARE) with * descriptor table being currently shared * 'to' being above the current capacity of descriptor table * 'from' being just under some chunk of opened descriptors. In that case we end up with observably wrong behaviour - e.g. spawn		

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
			a child with CLONE_FILES, get all descriptors in range 0..127 open, then close_range(64, ~0U, CLOSE_RANGE_UNSHARE) and watch dup(0) ending up with descriptor #128, despite #64 being observably not open. The minimally invasive fix would be to deal with that in dup_fd(). If this proves to add measurable overhead, we can go that way, but let's try to fix copy_fd_bitmaps() first. * new helper: bitmap_copy_and_expand(to, from, bits_to_copy, size). * make copy_fd_bitmaps() take the bitmap size in words, rather than bits; it's 'count' argument is always a multiple of BITS_PER_LONG,		

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
			so we are not losing any information, and that way we can use the same helper for all three bitmaps - compiler will see that count is a multiple of BITS_PER_LONG for the large ones, so it'll generate plain memcpy()+memset(). Reproducer added to tools/testing/selftests/core/close_range_test.c **CVE ID: CVE-2024-45025**		
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mmc: mmc_test: Fix NULL dereference on allocation failure If the "test->highmem = alloc_pages()" allocation fails then calling __free_pages(test->highmem) will	https://git.kernel.org/stable/c/2b507b03991f44dfb202fc2a82c9874d1b1f0c06, https://git.kernel.org/stable/c/3b4e76ceae5b5a46c968bd952f551ce173809f63, https://git.kernel.org/stable/c/9b9ba386d7bfdbc38445932c90fa9444c0524bea	O-LIN-LINU-190924/3365

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
			result in a NULL dereference. Also change the error code to -ENOMEM instead of returning success. **CVE ID: CVE-2024-45028**		
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: gtp: fix a potential NULL pointer dereference When sockfd_lookup() fails, gtp_encap_enable_socket() returns a NULL pointer, but its callers only check for error pointers thus miss the NULL pointer case. Fix it by returning an error pointer with the error code carried from sockfd_lookup(). (I found this bug during code inspection.)	https://git.kernel.org/stable/c/28c67f0f84f889fe9f4cbda8354132b20dc9212d, https://git.kernel.org/stable/c/4643b91691e969b1b9ad54bf552d7a990cfa3b87, https://git.kernel.org/stable/c/612edd35f2a3910ab1f61c1f2338889d4ba99fa2	O-LIN-LINU-190924/3366

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
			CVE ID: CVE-2024-46677		
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: pinctrl: single: fix potential NULL dereference in pcs_get_function() pinmux_generic_get_function() can return NULL and the pointer 'function' was dereferenced without checking against NULL. Add checking of pointer 'function' in pcs_get_function(). Found by code review. **CVE ID: CVE-2024-46685**	https://git.kernel.org/stable/c/0a2bab5ed161318f57134716acba0a30f3af191, https://git.kernel.org/stable/c/1c38a62f15e595346a1106025722869e87ffe044, https://git.kernel.org/stable/c/292151af6add3e5ab11b2e9916cffa5f52859a1f	O-LIN-LINU-190924/3367
Affected Version(s): From (including) 5.7 Up to (excluding) 6.6.48					
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: avoid possible UaF when selecting endp	https://git.kernel.org/stable/c/0201d65d9806d287a00e0ba96f0321835631f63f, https://git.kernel.org/stable/c/48e50dcbcbaaf713d82bf2da5c16aeced94ad07	O-LIN-LINU-190924/3368

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
			select_local_address() and select_signal_address() both select an endpoint entry from the list inside an RCU protected section, but return a reference to it, to be read later on. If the entry is dereferenced after the RCU unlock, reading info could cause a Use-after-Free. A simple solution is to copy the required info while inside the RCU protected section to avoid any risk of UaF later. The address ID might need to be modified later to handle the ID0 case later, so a copy seems OK to deal with. **CVE ID: CVE-2024-44974**	d, https://git.kernel.org/stable/c/9a9afbbc3fbfca4975eea4aa5b18556db5a0c0b8	
Affected Version(s): From (including) 5.9 Up to (excluding) 5.10.225					
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bonding: fix xfrm real_dev null	https://git.kernel.org/stable/c/21816b696c172c19d53a30d45ee005cce246ed21, https://git.kern	O-LIN-LINU-190924/3369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pointer dereference We shouldn't set real_dev to NULL because packets can be in transit and xfrm might call xdo_dev_offload_ok() in parallel. All callbacks assume real_dev is set. Example trace: kernel: BUG: unable to handle page fault for address: 0000000000001030 kernel: bond0: (slave eni0np1): making interface the new active one kernel: #PF: supervisor write access in kernel mode kernel: #PF: error_code(0x0002) - not-present page kernel: PGD 0 P4D 0 kernel: Oops: 0002 [#1] PREEMPT SMP kernel: CPU: 4 PID: 2237 Comm: ping	el.org/stable/c/2f72c6a66bcd7e0187ec085237fee5db27145294, https://git.kernel.org/stable/c/4582d4ff413a07d4ed8a4823c652dc5207760548	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Not tainted 6.7.7+ #12 kernel: Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 kernel: RIP: 0010:nsim_ipsec_offload_ok+0xc/0x20 [netdevsim] kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: Code: e0 0f 0b 48 83 7f 38 00 74 de 0f 0b 48 8b 47 08 48 8b 37 48 8b 78 40 e9 b2 e5 9a d7 66 90 0f 1f 44 00 00 48 8b 86 80 02 00 00 <83> 80 30 10 00 00 01 b8 01 00 00 00 c3 0f 1f 80 00 00 00 00 0f 1f kernel: bond0: (slave eni0np1): making interface the new active one kernel: RSP: 0018:ffffabde81553b98 EFLAGS: 00010246 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel:		

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
			kernel: RAX: 0000000000000000 RBX: ffff9eb404e74900 RCX: ffff9eb403d97c60 kernel: RDX: ffffffffc090de10 RSI: ffff9eb404e74900 RDI: ffff9eb3c5de9e00 kernel: RBP: ffff9eb3c0a42000 R08: 0000000000000010 R09: 0000000000000014 kernel: R10: 7974203030303030 R11: 3030303030303030 R12: 0000000000000000 kernel: R13: ffff9eb3c5de9e00 R14: ffffabde81553cc8 R15: ffff9eb404c53000 kernel: FS: 00007f2a77a3ad00(0000) GS:ffff9eb43bd00000(0000) knlGS:0000000000000000 kernel: CS: 0010 DS: 0000 ES: 0000 CR0:		

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
			0000000080050033 kernel: CR2: 0000000000001030 CR3: 00000001122ab000 CR4: 0000000000350ef0 kernel: bond0: (slave eni0np1): making interface the new active one kernel: Call Trace: kernel: <TASK> kernel: ? __die+0x1f/0x60 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ? page_fault_oops+0x142/0x4c0 kernel: ? do_user_addr_fault+0x65/0x670 kernel: ? kvm_read_and_reset_apf_flags+0x3b/0x50 kernel: bond0: (slave eni0np1): making interface the new active one kernel: ? exc_page_fault+0x7b/0x180		

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
			kernel: ? asm_exc_page_fault +0x22/0x30 kernel: ? nsim_bpf_uninit+0 x50/0x50 [netdevsim] kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_ all: failed to add SA kernel: ? nsim_ipsec_offload_ ok+0xc/0x20 [netdevsim] kernel: bond0: (slave eni0np1): making interface the new active one kernel: bond_ipsec_offload _ok+0x7b/0x90 [bonding] kernel: xfrm_output+0x61 /0x3b0 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_ all: failed to add SA kernel: ip_push_pending_fr ames+0x56/0x80 **CVE ID: CVE-2024-44989**		
NULL Pointer Dereferenc e	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kern el.org/stable/c/ 0707260a1831 2bbcd2a566858 4e3692d0a29e3 f6,	O-LIN-LINU-190924/3370

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
			bonding: fix null pointer deref in bond_ipsec_offload_ok We must check if there is an active slave before dereferencing the pointer. **CVE ID: CVE-2024-44990**	https://git.kernel.org/stable/c/2f5bdd68c1ce64bda6bef4d361a3de23b04ccd59, https://git.kernel.org/stable/c/32a0173600c63aadaf2103bf02f074982e8602ab	
Affected Version(s): From (including) 6.1.16 Up to (excluding) 6.1.108					
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: smb/client: avoid dereferencing rdata=NULL in smb2_new_read_req() This happens when called from SMB2_read() while using rdma and reaching the rdma_readwrite_threshold. **CVE ID: CVE-2024-46686**	https://git.kernel.org/stable/c/6df57c63c200cd05e085c3b695128260e21959b7, https://git.kernel.org/stable/c/a01859dd6aebf826576513850a3b05992809e9d2, https://git.kernel.org/stable/c/b902fb78ab21299e4dd1775e7e8d251d5c0735bc	O-LIN-LINU-190924/3371
Affected Version(s): From (including) 6.1.69 Up to (excluding) 6.1.107					
Improper Locking	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/03d3734bd692affe4d0e9c9d638f491aaf37411b,	O-LIN-LINU-190924/3372

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
			net/mlx5e: Take state lock during tx timeout reporter mlx5e_safe_reopen_channels() requires the state lock taken. The referenced changed in the Fixes tag removed the lock to fix another issue. This patch adds it back but at a later point (when calling mlx5e_safe_reopen_channels()) to avoid the deadlock referenced in the Fixes tag. **CVE ID: CVE-2024-45019**	https://git.kernel.org/stable/c/8e57e66ecbdd2fddc9fbf3e984b1c523b70e9809, https://git.kernel.org/stable/c/b3b9a87adee97854bcd71057901d46943076267e	
Affected Version(s): From (including) 6.1.95 Up to (excluding) 6.1.105					
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: driver core: Fix uevent_show() vs driver detach race uevent_show() wants to de-reference dev->driver->name. There is no clean	https://git.kernel.org/stable/c/15fffc6a5624b13b428bb1c6e9088e32a55eb82c, https://git.kernel.org/stable/c/49ea4e0d862632d51667da5e7a9c88a560e9c5a1, https://git.kernel.org/stable/c/4a7c2a8387524942171037e70	O-LIN-LINU-190924/3373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			way for a device attribute to de-reference dev->driver unless that attribute is defined via (struct device_driver).dev_groups. Instead, the anti-pattern of taking the device_lock() in the attribute handler risks deadlocks with code paths that remove device attributes while holding the lock. This deadlock is typically invisible to lockdep given the device_lock() is marked lockdep_set_novalidate_class(), but some subsystems allocate a local lockdep key for @dev->mutex to reveal reports of the form: ========== ========== ========== =========	b80e969c3b5c05b	

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
			WARNING: possible circular locking dependency detected 6.10.0-rc7+ #275 Tainted: G OE N --- modprobe/2374 is trying to acquire lock: ffff8c2270070de0 (kn->active#6){++++}-{0:0}, at: __kernfs_remove+0xde/0x220 but task is already holding lock: ffff8c22016e88f8 (&cxl_root_key){+.+.}-{3:3}, at: device_release_driver_internal+0x39/0x210 which lock already depends on the new lock. the existing dependency chain (in reverse order) is:		

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
			-> #1 (&cxl_root_key){+.+.}-{3:3}: __mutex_lock+0x99/0xc30 uevent_show+0xac/0x130 dev_attr_show+0x18/0x40 sysfs_kf_seq_show+0xac/0xf0 seq_read_iter+0x110/0x450 vfs_read+0x25b/0x340 ksys_read+0x67/0xf0 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e -> #0 (kn->active#6){++++}-{0:0}: __lock_acquire+0x121a/0x1fa0		

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
			lock_acquire+0xd6/0x2e0 kernfs_drain+0x1e9/0x200 __kernfs_remove+0xde/0x220 kernfs_remove_by_name_ns+0x5e/0xa0 device_del+0x168/0x410 device_unregister+0x13/0x60 devres_release_all+0xb8/0x110 device_unbind_cleanup+0xe/0x70 device_release_driver_internal+0x1c7/0x210 driver_detach+0x47/0x90 bus_remove_driver+0x6c/0xf0 cxl_acpi_exit+0xc/0x11 [cxl_acpi] __do_sys_delete_mo		

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
			dule.isra.0+0x181/0x260 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e The observation though is that driver objects are typically much longer lived than device objects. It is reasonable to perform lockless de-reference of a @driver pointer even if it is racing detach from a device. Given the infrequency of driver unregistration, use synchronize_rcu() in module_remove_driver() to close any potential races. It is potentially overkill to suffer synchronize_rcu() just to handle the rare module removal racing		

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
			uevent_show() event. Thanks to Tetsuo Handa for the debug analysis of the syzbot report [1]. **CVE ID: CVE-2024-44952**		
Affected Version(s): From (including) 6.1.95 Up to (excluding) 6.1.107					
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/vmalloc: fix page mapping if vm_area_alloc_pages() with high order fallback to order 0 The __vmap_pages_range_noflush() assumes its argument pages** contains pages with the same page shift. However, since commit e9c3cda4d86e ("mm, vmalloc: fix high order __GFP_NOFAIL allocations"), if gfp_flags includes	https://git.kernel.org/stable/c/61ebe5a747da649057c37be1c37eb934b4af79ca, https://git.kernel.org/stable/c/c91618816f4d21fc574d7577a37722adcd4075b2, https://git.kernel.org/stable/c/de7bad86345c43cd040ed43e20d9fad78a3ee59f	O-LIN-LINU-190924/3374

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
			__GFP_NOFAIL with high order in vm_area_alloc_pages() and page allocation failed for high order, the pages** may contain two different page shifts (high order and order-0). This could lead __vmap_pages_range_noflush() to perform incorrect mappings, potentially resulting in memory corruption. Users might encounter this as follows (vmap_allow_huge = true, 2M is for PMD_SIZE): kvmalloc(2M, __GFP_NOFAIL|GFP_X) __vmalloc_node_range_noprof(vm_flags=VM_ALLOW_HUGE_VMAP) vm_area_alloc_pages(order=9) ---> order-9 allocation		

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
			failed and fallback to order-0 vmap_pages_range() vmap_pages_range_noflush() __vmap_pages_range_noflush(page_shift = 21) ----> wrong mapping happens We can remove the fallback code because if a high-order allocation fails, __vmalloc_node_range_noprof() will retry with order-0. Therefore, it is unnecessary to fallback to order-0 here. Therefore, fix this by removing the fallback code. **CVE ID: CVE-2024-45022**		
Affected Version(s): From (including) 6.10 Up to (excluding) 6.10.5					
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: driver core: Fix uevent_show() vs driver detach race	https://git.kernel.org/stable/c/15fffc6a5624b13b428bb1c6e9088e32a55eb82c, https://git.kernel.org/stable/c/49ea4e0d86263	O-LIN-LINU-190924/3375

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
			uevent_show() wants to de-reference dev->driver->name. There is no clean way for a device attribute to de-reference dev->driver unless that attribute is defined via (struct device_driver).dev_groups. Instead, the anti-pattern of taking the device_lock() in the attribute handler risks deadlocks with code paths that remove device attributes while holding the lock. This deadlock is typically invisible to lockdep given the device_lock() is marked lockdep_set_novalidate_class(), but some subsystems allocate a local lockdep key for @dev->mutex to reveal reports of the form:	2d51667da5e7a9c88a560e9c5a1, https://git.kernel.org/stable/c/4a7c2a8387524942171037e70b80e969c3b5c05b	

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
			========== ========== ========== ========= WARNING: possible circular locking dependency detected 6.10.0-rc7+ #275 Tainted: G OE N ---------- ---------- ----- modprobe/2374 is trying to acquire lock: ffff8c2270070de0 (kn->active#6){++++}-{0:0}, at: __kernfs_remove+0xde/0x220 but task is already holding lock: ffff8c22016e88f8 (&cxl_root_key){+.+.}-{3:3}, at: device_release_driver_internal+0x39/0x210 which lock already depends on the new lock.		

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 existing dependency chain (in reverse order) is: -> #1 (&cxl_root_key){+.+.}-{3:3}: __mutex_lock+0x99/0xc30 uevent_show+0xac/0x130 dev_attr_show+0x18/0x40 sysfs_kf_seq_show+0xac/0xf0 seq_read_iter+0x110/0x450 vfs_read+0x25b/0x340 ksys_read+0x67/0xf0 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e		

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 (kn->active#6){++++}-{0:0}: __lock_acquire+0x121a/0x1fa0 lock_acquire+0xd6/0x2e0 kernfs_drain+0x1e9/0x200 __kernfs_remove+0xde/0x220 kernfs_remove_by_name_ns+0x5e/0xa0 device_del+0x168/0x410 device_unregister+0x13/0x60 devres_release_all+0xb8/0x110 device_unbind_cleanup+0xe/0x70 device_release_driver_internal+0x1c7/0x210 driver_detach+0x47/0x90		

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
			bus_remove_driver+0x6c/0xf0 cxl_acpi_exit+0xc/0x11 [cxl_acpi] __do_sys_delete_module.isra.0+0x181/0x260 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e The observation though is that driver objects are typically much longer lived than device objects. It is reasonable to perform lockless de-reference of a @driver pointer even if it is racing detach from a device. Given the infrequency of driver unregistration, use synchronize_rcu() in module_remove_driver() to close any potential		

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
			races. It is potentially overkill to suffer synchronize_rcu() just to handle the rare module removal racing uevent_show() event. Thanks to Tetsuo Handa for the debug analysis of the syzbot report [1]. **CVE ID: CVE-2024-44952**		
Affected Version(s): From (including) 6.10 Up to (excluding) 6.10.7					
Integer Overflow or Wraparound	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: workqueue: Fix UBSAN 'subtraction overflow' error in shift_and_mask() UBSAN reports the following 'subtraction overflow' error when booting in a virtual machine on Android: | Internal error: UBSAN: integer subtraction	https://git.kernel.org/stable/c/38f7e14519d39cf524ddc02d4caee9b337dad703, https://git.kernel.org/stable/c/90a6a844b2d9927d192758438a4ada33d8cd9de5	O-LIN-LINU-190924/3376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow: 00000000f2005515 [#1] PREEMPT SMP | Modules linked in: | CPU: 0 PID: 1 Comm: swapper/0 Not tainted 6.10.0-00006-g3cbe9e5abd46-dirty #4 | Hardware name: linux,dummy-virt (DT) | pstate: 600000c5 (nZCv daIF -PAN -UAO -TCO -DIT -SSBS BTYPE=--) | pc : cancel_delayed_work+0x34/0x44 | lr : cancel_delayed_work+0x2c/0x44 | sp : ffff80008002ba60 | x29: ffff80008002ba60 x28: 0000000000000000 x27: 0000000000000000 | x26: 0000000000000000 x25: 0000000000000000 x24: 0000000000000000		

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
			| x23: 0000000000000000 x22: 0000000000000000 x21: ffff1f65014cd3c0 | x20: ffffc0e84c9d0da0 x19: ffffc0e84cab3558 x18: ffff800080009058 | x17: 00000000247ee1f8 x16: 00000000247ee1f8 x15: 00000000bdcb279d | x14: 0000000000000001 x13: 0000000000000075 x12: 00000a0000000000 | x11: ffff1f6501499018 x10: 00984901651fffff x9 : ffff5e7cc35af000 | x8 : 0000000000000001 x7 : 3d4d455453595342 x6 : 000000004e514553 | x5 : ffff1f6501499265 x4 :		

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
			ffff1f650ff60b10 x3 : 0000000000000620 | x2 : ffff80008002ba78 x1 : 0000000000000000 x0 : 0000000000000000 | Call trace: | cancel_delayed_work+0x34/0x44 | deferred_probe_extend_timeout+0x20/0x70 | driver_register+0xa8/0x110 | __platform_driver_register+0x28/0x3c | syscon_init+0x24/0x38 | do_one_initcall+0xe4/0x338 | do_initcall_level+0xac/0x178 | do_initcalls+0x5c/0xa0 | do_basic_setup+0x20/0x30		

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
			| kernel_init_freeable+0x8c/0xf8 | kernel_init+0x28/0x1b4 | ret_from_fork+0x10/0x20 | Code: f9000fbf 97fffa2f 39400268 37100048 (d42aa2a0) | ---[end trace 0000000000000000]--- | Kernel panic - not syncing: UBSAN: integer subtraction overflow: Fatal exception This is due to shift_and_mask() using a signed immediate to construct the mask and being called with a shift of 31 (WORK_OFFQ_POOL_SHIFT) so that it ends up decrementing from INT_MIN. Use an unsigned constant '1U' to generate the mask		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in shift_and_mask(). **CVE ID: CVE-2024-44981**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: smb/client: avoid possible NULL dereference in cifs_free_subrequest() Clang static checker (scan-build) warning: cifsglob.h:line 890, column 3 Access to field 'ops' results in a dereference of a null pointer. Commit 519be989717c ("cifs: Add a tracepoint to track credits involved in R/W requests") adds a check for 'rdata->server', and let clang throw this warning about NULL dereference. When 'rdata->credits.value != 0	https://git.kernel.org/stable/c/74c2ab6d653b4c2354df65a7f7f2df1925a40a51, https://git.kernel.org/stable/c/fead60a6d5f84b472b928502a42c419253afe6c1	O-LIN-LINU-190924/3377

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
			&& rdata->server == NULL' happens, add_credits_and_wake_if() will call rdata->server->ops->add_credits(). This will cause NULL dereference problem. Add a check for 'rdata->server' to avoid NULL dereference. **CVE ID: CVE-2024-44992**		
Allocation of Resources Without Limits or Throttling	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: s390/boot: Avoid possible physmem_info segment corruption When physical memory for the kernel image is allocated it does not consider extra memory required for offsetting the image start to match it with the lower 20 bits of KASLR virtual base address. That	https://git.kernel.org/stable/c/a944cba5d57687b747023c3bc074fcf9c790f7df, https://git.kernel.org/stable/c/d7fd2941ae9a67423d1c7bee985f240e4686634f	O-LIN-LINU-190924/3378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			might lead to kernel access beyond its memory range. **CVE ID: CVE-2024-45014**		
Improper Locking	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: fix hugetlb vs. core-mm PT locking We recently made GUP's common page table walking code to also walk hugetlb VMAs without most hugetlb special-casing, preparing for the future of having less hugetlb-specific page table walking code in the codebase. Turns out that we missed one page table locking detail: page table locking for hugetlb folios that are not mapped using a single PMD/PUD. Assume we have hugetlb folio that	https://git.kernel.org/stable/c/5f75cfbd6bb02295ddaed48adf667b6c828ce07b, https://git.kernel.org/stable/c/7300dadba49e531af2d890ae4e34c9b115384a62	O-LIN-LINU-190924/3379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			spans multiple PTEs (e.g., 64 KiB hugetlb folios on arm64 with 4 KiB base page size). GUP, as it walks the page tables, will perform a pte_offset_map_lock() to grab the PTE table lock. However, hugetlb that concurrently modifies these page tables would actually grab the mm->page_table_lock: with USE_SPLIT_PTE_PTLOCKS, the locks would differ. Something similar can happen right now with hugetlb folios that span multiple PMDs when USE_SPLIT_PMD_PTLOCKS. This issue can be reproduced [1], for example triggering: [3105.936100] ------------[cut here]------------		

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
			[3105.939323] WARNING: CPU: 31 PID: 2732 at mm/gup.c:142 try_grab_folio+0x11c/0x188 [3105.944634] Modules linked in: [...] [3105.974841] CPU: 31 PID: 2732 Comm: reproducer Not tainted 6.10.0-64.eln141.aarch64 #1 [3105.980406] Hardware name: QEMU KVM Virtual Machine, BIOS edk2-20240524-4.fc40 05/24/2024 [3105.986185] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [3105.991108] pc : try_grab_folio+0x11c/0x188 [3105.994013] lr : follow_page_pte+0xd8/0x430 [3105.996986] sp : ffff80008eafb8f0 [3105.999346] x29: ffff80008eafb900 x28: ffffffe8d481f380 x27: 00f80001207cff43		

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
			[3106.004414] x26: 0000000000000001 x25: 0000000000000000 x24: ffff80008eafba48 [3106.009520] x23: 0000ffff9372f000 x22: ffff7a54459e2000 x21: ffff7a546c1aa978 [3106.014529] x20: ffffffe8d481f3c0 x19: 0000000000610041 x18: 0000000000000001 [3106.019506] x17: 0000000000000001 x16: ffffffffffffffff x15: 0000000000000000 [3106.024494] x14: ffffb85477fdfe08 x13: 0000ffff9372ffff x12: 0000000000000000 [3106.029469] x11: 1fffef4a88a96be1 x10: ffff7a54454b5f0c		

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
			x9 : ffffb854771b12f0 [3106.034324] x8 : 0008000000000000 x7 : ffff7a546c1aa980 x6 : 0008000000000080 [3106.038902] x5 : 00000000001207cf x4 : 0000ffff9372f000 x3 : ffffffe8d481f000 [3106.043420] x2 : 0000000000610041 x1 : 0000000000000001 x0 : 0000000000000000 [3106.047957] Call trace: [3106.049522] try_grab_folio+0x11c/0x188 [3106.051996] follow_pmd_mask.constprop.0.isra.0+0x150/0x2e0 [3106.055527] follow_page_mask+0x1a0/0x2b8 [3106.058118] __get_user_pages+0xf0/0x348 [3106.060647] faultin_page_range+0xb0/0x360		

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
			[3106.063651] do_madvise+0x340 /0x598 Let's make huge_pte_lockptr() effectively use the same PT locks as any core-mm page table walker would. Add ptep_lockptr() to obtain the PTE page table lock using a pte pointer -- unfortunately we cannot convert pte_lockptr() because virt_to_page() doesn't work with kmap'ed page tables we can have with CONFIG_HIGHPTE. Handle CONFIG_PGTABLE_LEVELS correctly by checking in reverse order, such that when e.g., CONFIG_PGTABLE_LEVELS==2 with PGDIR_SIZE==P4D_SIZE==PUD_SIZE==PMD_SIZE will work as expected. Document why that works.		

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
			There is one ugly case: powerpc 8xx, whereby we have an 8 MiB hugetlb folio being mapped using two PTE page tables. While hugetlb wants to take the PMD table lock, core-mm would grab the PTE table lock of one of both PTE page tables. In such corner cases, we have to make sure that both locks match, which is (fortunately!) currently guaranteed for 8xx as it does not support SMP and consequently doesn't use split PT locks. [1] https://lore.kernel.org/all/1bbfcc7f-f222-45a5-ac44-c5a1381c596d@redhat.com/ **CVE ID: CVE-2024-45024**		
Affected Version(s): From (including) 6.10 Up to (excluding) 6.10.8					
Use After Free	13-Sep-2024	7.8	In the Linux kernel, the following	https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3380

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
			vulnerability has been resolved: drm/xe: prevent UAF around preempt fence The fence lock is part of the queue, therefore in the current design anything locking the fence should then also hold a ref to the queue to prevent the queue from being freed. However, currently it looks like we signal the fence and then drop the queue ref, but if something is waiting on the fence, the waiter is kicked to wake up at some later point, where upon waking up it first grabs the lock before checking the fence state. But if we have already dropped the queue ref, then the lock might already be freed as part of	10081b0b0ed201f53e24bd92deb2e0f3c3e713d4, https://git.kernel.org/stable/c/730b72480e29f63fd644f5fa57c9d46109428953	

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 queue, leading to uaf. To prevent this, move the fence lock into the fence itself so we don't run into lifetime issues. Alternative might be to have device level lock, or only release the queue in the fence release callback, however that might require pushing to another worker to avoid locking issues. References: https://gitlab.freedesktop.org/drm/xe/kernel/-/issues/2454 References: https://gitlab.freedesktop.org/drm/xe/kernel/-/issues/2342 References: https://gitlab.freedesktop.org/drm/xe/kernel/-/issues/2020 (cherry picked from commit 7116c35aacedc38be6d15bd21b2fc936eed0008b)		

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
			CVE ID: CVE-2024-46683		
N/A	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Disable preemption while updating GPU stats We forgot to disable preemption around the write_seqcount_begin/end() pair while updating GPU stats: [ ] WARNING: CPU: 2 PID: 12 at include/linux/seqlock.h:221 __seqprop_assert.isra.0+0x128/0x150 [v3d] [ ] Workqueue: v3d_bin drm_sched_run_job_work [gpu_sched] <...snip...> [ ] Call trace: [ ] __seqprop_assert.isra.0+0x128/0x150 [v3d] [ ] v3d_job_start_stats.	https://git.kernel.org/stable/c/1e93467ef20308da5a94cde548ee17d523e8ba7b, https://git.kernel.org/stable/c/9d824c7fce58f59982228aa85b0376b113cdfa35	O-LIN-LINU-190924/3381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			isra.0+0x90/0x218 [v3d] [ ] v3d_bin_job_run+0x23c/0x388 [v3d] [ ] drm_sched_run_job_work+0x520/0x6d0 [gpu_sched] [ ] process_one_work+0x62c/0xb48 [ ] worker_thread+0x468/0x5b0 [ ] kthread+0x1c4/0x1e0 [ ] ret_from_fork+0x10/0x20 Fix it. **CVE ID: CVE-2024-46699**		
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: typec: ucsi: Move unregister out of atomic section Commit '9329933699b3 ("soc: qcom:	https://git.kernel.org/stable/c/095b0001aefddcd9361097c971b7debc84e72714, https://git.kernel.org/stable/c/11bb2ffb679399f99041540cf662409905179e3a	O-LIN-LINU-190924/3382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pmic_glink: Make client-lock non-sleeping")' moved the pmic_glink client list under a spinlock, as it is accessed by the rpmsg/glink callback, which in turn is invoked from IRQ context. This means that ucsi_unregister() is now called from atomic context, which isn't feasible as it's expecting a sleepable context. An effort is under way to get GLINK to invoke its callbacks in a sleepable context, but until then lets schedule the unregistration. A side effect of this is that ucsi_unregister() can now happen after the remote processor, and thereby the communication link with it, is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gone. pmic_glink_send() is amended with a check to avoid the resulting NULL pointer dereference. This does however result in the user being informed about this error by the following entry in the kernel log: ucsi_glink.pmic_glink_ucsi pmic_glink.ucsi.0: failed to send UCSI write request: -5 **CVE ID: CVE-2024-46691**		
Affected Version(s): From (including) 6.2 Up to (excluding) 6.5.5					
NULL Pointer Dereference	06-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: media: dvb-usb-v2: af9035: Fix null-ptr-deref in af9035_i2c_master_xfer In af9035_i2c_master_xfer, msg is controlled by user. When msg[i].buf	https://git.kernel.org/stable/c/0143f282b15f7cedc0392ea10050fb6000fd16e6, https://git.kernel.org/stable/c/41b7181a40af84448a2b144fb02d8bf32b7e9a23, https://git.kernel.org/stable/c/6c01ef65de0b321b2db1ef9abf8f1d15862b937e	O-LIN-LINU-190924/3383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is null and msg[i].len is zero, former checks on msg[i].buf would be passed. Malicious data finally reach af9035_i2c_master_xfer. If accessing msg[i].buf[0] without sanity check, null ptr deref would happen. We add check on msg[i].len to prevent crash. Similar commit: commit 0ed554fd769a ("media: dvb-usb: az6027: fix null-ptr-deref in az6027_i2c_xfer()") **CVE ID: CVE-2023-52915**		
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.46					
Missing Release of Memory after Effective Lifetime	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: dsa: bcm_sf2: Fix a possible memory leak in bcm_sf2_mdio_register()	https://git.kernel.org/stable/c/7feef10768ea71d468d9bbc1e0d14c461876768c, https://git.kernel.org/stable/c/a7d2808d67570e6acae45c2a96e0d59986888e4c, https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bcm_sf2_mdio_register() calls of_phy_find_device() and then phy_device_remove() in a loop to remove existing PHY devices. of_phy_find_device() eventually calls bus_find_device(), which calls get_device() on the returned struct device * to increment the refcount. The current implementation does not decrement the refcount, which causes memory leak. This commit adds the missing phy_device_free() call to decrement the refcount via put_device() to balance the refcount. **CVE ID: CVE-2024-44971**	b7b8d9f5e679af60c94251fd6728dde34be69a71	
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.48					
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/124b428fe28064c809e4237b0b	O-LIN-LINU-190924/3385

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
			ipv6: prevent possible UAF in ip6_xmit() If skb_expand_head() returns NULL, skb has been freed and the associated dst/idev could also have been freed. We must use rcu_read_lock() to prevent a possible UAF. **CVE ID: CVE-2024-44985**	38e97200a8a4a8, https://git.kernel.org/stable/c/2d5ff7e339d04622d8282661df36151906d0e1c7, https://git.kernel.org/stable/c/38a21c026ed2cc7232414cb166efc1923f34af17	
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: ipv6: fix possible UAF in ip6_finish_output2() If skb_expand_head() returns NULL, skb has been freed and associated dst/idev could also have been freed. We need to hold rcu_read_lock() to	https://git.kernel.org/stable/c/3574d28caf9a09756ae87ad1ea096c6f47b6101e, https://git.kernel.org/stable/c/56efc253196751ece1fc535a5b582be127b0578a, https://git.kernel.org/stable/c/6ab6bf731354a6fdbaa617d1ec194960db61cf3b	O-LIN-LINU-190924/3386

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
			make sure the dst and associated idev are alive. **CVE ID: CVE-2024-44986**		
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent UAF in ip6_send_skb() syzbot reported an UAF in ip6_send_skb() [1] After ip6_local_out() has returned, we no longer can safely dereference rt, unless we hold rcu_read_lock(). A similar issue has been fixed in commit a688caa34beb ("ipv6: take rcu lock in rawv6_send_hdrinc()") Another potential issue in ip6_finish_output2() is handled in a	https://git.kernel.org/stable/c/24e93695b1239fbe4c31e224372be77f82dab69a, https://git.kernel.org/stable/c/571567e0277008459750f0728f246086b2659429, https://git.kernel.org/stable/c/9a3e55afa95ed4ac9eda112d4f918af645d72f25	O-LIN-LINU-190924/3387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			separate patch. [1] BUG: KASAN: slab-use-after-free in ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 Read of size 8 at addr ffff88806dde4858 by task syz.1.380/6530 CPU: 1 UID: 0 PID: 6530 Comm: syz.1.380 Not tainted 6.11.0-rc3-syzkaller-00306-gdf6cbc62cc9b #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/06/2024 Call Trace: <TASK> __dump_stack lib/dump_stack.c:93 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:119 print_address_desc		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ription mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x143/0x180 mm/kasan/report.c:601 ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 rawv6_push_pending_frames+0x75c/0x9e0 net/ipv6/raw.c:588 rawv6_sendmsg+0x19c7/0x23c0 net/ipv6/raw.c:926 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 sock_write_iter+0x2dd/0x400 net/socket.c:1160		

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
			do_iter_readv_writev+0x60a/0x890 vfs_writev+0x37c/0xbb0 fs/read_write.c:971 do_writev+0x1b1/0x350 fs/read_write.c:1018 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f936bf79e79 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 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 a8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f936cd7f038 EFLAGS:		

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
			00000246 ORIG_RAX: 0000000000000014 RAX: ffffffffffffffda RBX: 00007f936c115f80 RCX: 00007f936bf79e79 RDX: 0000000000000001 RSI: 0000000020000040 RDI: 0000000000000004 RBP: 00007f936bfe7916 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000000 R14: 00007f936c115f80 R15: 00007fff2860a7a8 </TASK> Allocated by task 6530:		

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
			kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 unpoison_slab_object mm/kasan/common.c:312 [inline] __kasan_slab_alloc+0x66/0x80 mm/kasan/common.c:338 kasan_slab_alloc include/linux/kasan.h:201 [inline] slab_post_alloc_hook mm/slub.c:3988 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_noprof+0x135/0x2a0 mm/slub.c:4044 dst_alloc+0x12b/0x190 net/core/dst.c:89 ip6_blackhole_route+0x59/0x340 net/ipv6/route.c:2670		

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
			make_blackhole net/xfrm/xfrm_policy.c:3120 [inline] xfrm_lookup_route+0xd1/0x1c0 net/xfrm/xfrm_policy.c:3313 ip6_dst_lookup_flow+0x13e/0x180 net/ipv6/ip6_output.c:1257 rawv6_sendmsg+0x1283/0x23c0 net/ipv6/raw.c:898 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 ___sys_sendmsg+0x525/0x7d0 net/socket.c:2597 ___sys_sendmsg net/socket.c:2651 [inline] __sys_sendmsg+0x2b0/0x3a0 net/socket.c:2680 do_syscall_x64 arch/x86/entry/common.c:52 [inline]		

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
			do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 45: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 kasan_save_free_info+0x40/0x50 mm/kasan/generic.c:579 poison_slab_object+0xe0/0x150 mm/kasan/common.c:240 __kasan_slab_free+0x37/0x60 mm/kasan/common.c:256 kasan_slab_free include/linux/kasan.h:184 [inline] slab_free_hook mm/slub.c:2252 [inline]		

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
			slab_free mm/slub.c:4473 [inline] kmem_cache_free+0x145/0x350 mm/slub.c:4548 dst_destroy+0x2ac/0x460 net/core/dst.c:124 rcu_do_batch kernel/rcu/tree.c:2569 [inline] rcu_core+0xafd/0x1830 kernel/rcu/tree. ---truncated--- **CVE ID: CVE-2024-44987**		
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: mtk_wed: fix use-after-free panic in mtk_wed_setup_tc_block_cb() When there are multiple ap interfaces on one band and with WED on, turning the interface down will	https://git.kernel.org/stable/c/326a89321f9d5fe399fe6f9ff7c0fc766582a6a0, https://git.kernel.org/stable/c/b453a4bbda03aa8741279c360ac82d1c3ac33548, https://git.kernel.org/stable/c/db1b4bedb9b97c6d34b03d03815147c04fffe8b4	O-LIN-LINU-190924/3388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a kernel panic on MT798X. Previously, cb_priv was freed in mtk_wed_setup_tc_block() without marking NULL,and mtk_wed_setup_tc_block_cb() didn't check the value, too. Assign NULL after free cb_priv in mtk_wed_setup_tc_block() and check NULL in mtk_wed_setup_tc_block_cb(). --------- Unable to handle kernel paging request at virtual address 0072460bca32b4f5 Call trace: mtk_wed_setup_tc_block_cb+0x4/0x38 0xffffffc0794084bc tcf_block_playback_offloads+0x70/0x1e8		

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
			tcf_block_unbind+0x6c/0xc8 ... --------- **CVE ID: CVE-2024-44997**		
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: atm: idt77252: prevent use after free in dequeue_rx() We can't dereference "skb" after calling vcc->push() because the skb is released. **CVE ID: CVE-2024-44998**	https://git.kernel.org/stable/c/09e086a5f72ea27c758b3f3b419a69000c32adc1, https://git.kernel.org/stable/c/1cece837e387c039225f19028df255df87a97c0d, https://git.kernel.org/stable/c/24cf390a5426aac9255205e9533cdd7b4235d518	O-LIN-LINU-190924/3389
Out-of-bounds Write	11-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: s390/dasd: fix error recovery leading to data corruption on ESE devices Extent Space Efficient (ESE) or	https://git.kernel.org/stable/c/0a228896a1b3654cd461ff654f6a64e97a9c3246, https://git.kernel.org/stable/c/19f60a55b2fda49bc4f6134a5f6356ef62ee69d8, https://git.kernel.org/stable/c/5d4a304338daf	O-LIN-LINU-190924/3390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			thin provisioned volumes need to be formatted on demand during usual IO processing. The dasd_ese_needs_format function checks for error codes that signal the non existence of a proper track format. The check for incorrect length is to imprecise since other error cases leading to transport of insufficient data also have this flag set. This might lead to data corruption in certain error cases for example during a storage server warmstart. Fix by removing the check for incorrect length and replacing by explicitly checking for invalid track format in transport mode.	83ace2887aaacafd66fe99ed5cc	

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
			Also remove the check for file protected since this is not a valid ESE handling case. **CVE ID: CVE-2024-45026**		
Use of Uninitialized Resource	04-Sep-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: validate vlan header Ensure there is sufficient room to access the protocol field of the VLAN header, validate it once before the flowtable lookup. ========== ========== ========== ======== BUG: KMSAN: uninit-value in nf_flow_offload_inet_hook+0x45a/0x5f0 net/netfilter/nf_flow_table_inet.c:32 nf_flow_offload_inet_hook+0x45a/0x5	https://git.kernel.org/stable/c/0279c35d242d037abeb73d60d06a6d1bb7f672d9, https://git.kernel.org/stable/c/043a18bb6cf16adaa2f8642acfde6e8956a9caaa, https://git.kernel.org/stable/c/6ea14ccb60c8ab829349979b22b58a941ec4a3ee	O-LIN-LINU-190924/3391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f0 net/netfilter/nf_flow_table_inet.c:32 nf_hook_entry_hookfn include/linux/netfilter.h:154 [inline] nf_hook_slow+0xf4/0x400 net/netfilter/core.c:626 nf_hook_ingress include/linux/netfilter_netdev.h:34 [inline] nf_ingress net/core/dev.c:5440 [inline] **CVE ID: CVE-2024-44983**		
Use of Uninitialized Resource	04-Sep-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: gtp: pull network headers in gtp_dev_xmit() syzbot/KMSAN reported use of uninit-value in get_dev_xmit() [1] We must make sure the IPv4 or Ipv6 header is pulled in skb->head	https://git.kernel.org/stable/c/137d565ab89ce3584503b443bc9e00d44f482593, https://git.kernel.org/stable/c/1f6b62392453d8f36685d19b761307a8c5617ac1, https://git.kernel.org/stable/c/34ba4f29f3d9eb52dee37512059efb2afd7e966f	O-LIN-LINU-190924/3392

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
			before accessing fields in them. Use pskb_inet_may_pull() to fix this issue. [1] BUG: KMSAN: uninit-value in ipv6_pdp_find drivers/net/gtp.c:220 [inline] BUG: KMSAN: uninit-value in gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] BUG: KMSAN: uninit-value in gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281 ipv6_pdp_find drivers/net/gtp.c:220 [inline] gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281 __netdev_start_xmit include/linux/netdevice.h:4913 [inline]		

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
			netdev_start_xmit include/linux/netdevice.h:4922 [inline] xmit_one net/core/dev.c:3580 [inline] dev_hard_start_xmit+0x247/0xa20 net/core/dev.c:3596 __dev_queue_xmit+0x358c/0x5610 net/core/dev.c:4423 dev_queue_xmit include/linux/netdevice.h:3105 [inline] packet_xmit+0x9c/0x6c0 net/packet/af_packet.c:276 packet_snd net/packet/af_packet.c:3145 [inline] packet_sendmsg+0x90e3/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+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
			x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hoo		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			k mm/slub.c:3994 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_node_noprof+0x6bf/0xb80 mm/slub.c:4080 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:583 __alloc_skb+0x363/0x7b0 net/core/skbuff.c:674 alloc_skb include/linux/skbuff.h:1320 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6526 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2815 packet_alloc_skb net/packet/af_packet.c:2994 [inline] packet_snd net/packet/af_packet.c:3088 [inline] packet_sendmsg+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
			x749c/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_		

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
			after_hwframe+0x77/0x7f CPU: 0 UID: 0 PID: 7115 Comm: syz.1.515 Not tainted 6.11.0-rc1-syzkaller-00043-g94ede2a3e913 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 **CVE ID: CVE-2024-44999**		
Improper Initialization	02-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fuse: Initialize beyond-EOF page contents before setting uptodate fuse_notify_store(), unlike fuse_do_readpage(), does not enable page zeroing (because it can be used to change partial page contents). So fuse_notify_store()	https://git.kernel.org/stable/c/18a067240817bee8a9360539af5d79a4bf5398a5, https://git.kernel.org/stable/c/33168db352c7b56ae18aa55c2cae1a1c5905d30e, https://git.kernel.org/stable/c/3c0da3d163eb32f1f91891efaade027fa9b245b9	O-LIN-LINU-190924/3393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			must be more careful to fully initialize page contents (including parts of the page that are beyond end-of-file) before marking the page uptodate. The current code can leave beyond-EOF page contents uninitialized, which makes these uninitialized page contents visible to userspace via mmap(). This is an information leak, but only affects systems which do not enable init-on-alloc (via CONFIG_INIT_ON_ALLOC_DEFAULT_ON=y or the corresponding kernel command line parameter). **CVE ID: CVE-2024-44947**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/21816b696c172c19d53a30d45ee005cce246e	O-LIN-LINU-190924/3394

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
			bonding: fix xfrm real_dev null pointer dereference We shouldn't set real_dev to NULL because packets can be in transit and xfrm might call xdo_dev_offload_ok() in parallel. All callbacks assume real_dev is set. Example trace: kernel: BUG: unable to handle page fault for address: 0000000000001030 kernel: bond0: (slave eni0np1): making interface the new active one kernel: #PF: supervisor write access in kernel mode kernel: #PF: error_code(0x0002) - not-present page kernel: PGD 0 P4D 0 kernel: Oops: 0002 [#1] PREEMPT SMP	d21, https://git.kernel.org/stable/c/2f72c6a66bcd7e0187ec085237fee5db27145294, https://git.kernel.org/stable/c/4582d4ff413a07d4ed8a4823c652dc5207760548	

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
			kernel: CPU: 4 PID: 2237 Comm: ping Not tainted 6.7.7+ #12 kernel: Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 kernel: RIP: 0010:nsim_ipsec_offload_ok+0xc/0x20 [netdevsim] kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: Code: e0 0f 0b 48 83 7f 38 00 74 de 0f 0b 48 8b 47 08 48 8b 37 48 8b 78 40 e9 b2 e5 9a d7 66 90 0f 1f 44 00 00 48 8b 86 80 02 00 00 <83> 80 30 10 00 00 01 b8 01 00 00 00 c3 0f 1f 80 00 00 00 00 0f 1f kernel: bond0: (slave eni0np1): making interface the new active one kernel: RSP: 0018:ffffabde8155 3b98 EFLAGS: 00010246 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA		

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
			kernel: kernel: RAX: 0000000000000000 RBX: ffff9eb404e74900 RCX: ffff9eb403d97c60 kernel: RDX: ffffffffc090de10 RSI: ffff9eb404e74900 RDI: ffff9eb3c5de9e00 kernel: RBP: ffff9eb3c0a42000 R08: 0000000000000010 R09: 0000000000000014 kernel: R10: 7974203030303030 R11: 3030303030303030 R12: 0000000000000000 kernel: R13: ffff9eb3c5de9e00 R14: ffffabde81553cc8 R15: ffff9eb404c53000 kernel: FS: 00007f2a77a3ad00(0000) GS:ffff9eb43bd00000(0000) knlGS:0000000000000000 kernel: CS: 0010 DS: 0000 ES: 0000		

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
			CR0: 0000000080050033 kernel: CR2: 0000000000001030 CR3: 00000001122ab000 CR4: 0000000000350ef0 kernel: bond0: (slave eni0np1): making interface the new active one kernel: Call Trace: kernel: <TASK> kernel: ? __die+0x1f/0x60 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ? page_fault_oops+0x142/0x4c0 kernel: ? do_user_addr_fault+0x65/0x670 kernel: ? kvm_read_and_reset_apf_flags+0x3b/0x50 kernel: bond0: (slave eni0np1): making interface the new active one kernel: ? exc_page_fault+0x7b/0x180		

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
			kernel: ? asm_exc_page_fault +0x22/0x30 kernel: ? nsim_bpf_uninit+0 x50/0x50 [netdevsim] kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_ all: failed to add SA kernel: ? nsim_ipsec_offload_ ok+0xc/0x20 [netdevsim] kernel: bond0: (slave eni0np1): making interface the new active one kernel: bond_ipsec_offload _ok+0x7b/0x90 [bonding] kernel: xfrm_output+0x61 /0x3b0 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_ all: failed to add SA kernel: ip_push_pending_fr ames+0x56/0x80 **CVE ID: CVE-2024-44989**		
NULL Pointer Dereferenc e	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kern el.org/stable/c/ 0707260a1831 2bbcd2a566858 4e3692d0a29e3 f6,	O-LIN-LINU-190924/3395

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
			bonding: fix null pointer deref in bond_ipsec_offload _ok We must check if there is an active slave before dereferencing the pointer. **CVE ID: CVE-2024-44990**	https://git.kernel.org/stable/c/2f5bdd68c1ce64bda6bef4d361a3de23b04ccd59, https://git.kernel.org/stable/c/32a0173600c63aadaf2103bf02f074982e8602ab	
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix a deadlock problem when config TC during resetting When config TC during the reset process, may cause a deadlock, the flow is as below: pf reset start | ▼ ..... setup tc | | ▼ ▼ DOWN: napi_disable()	https://git.kernel.org/stable/c/195918217448a6bb7f929d6a2ffffce9f1ece1cc, https://git.kernel.org/stable/c/67492d4d105c0a6321b00c393eec96b9a7a97a16, https://git.kernel.org/stable/c/6ae2b7d63cd056f363045eb65409143e16f23ae8	O-LIN-LINU-190924/3396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			napi_disable()(skip) | | ▼ ▼ .... | | ▼ | napi_enable() | ▼ UINIT: netif_napi_del() | ▼ ..... | ▼ INIT: netif_napi_add() | ▼ ..... global reset start | | ▼ ▼ UP: napi_enable()(skip) ..... | | ▼ ▼		

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
			..... napi_disable() In reset process, the driver will DOWN the port and then UINIT, in this case, the setup tc process will UP the port before UINIT, so cause the problem. Adds a DOWN process in UINIT to fix it. **CVE ID: CVE-2024-44995**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fs/netfs/fscache_cookie: add missing "n_accesses" check This fixes a NULL pointer dereference bug due to a data race which looks like this: BUG: kernel NULL pointer dereference, address: 0000000000000008	https://git.kernel.org/stable/c/0a4d41fa14b2a0efd40e350cfe8ec6a4c998ac1d, https://git.kernel.org/stable/c/b8a50877f68efdcc0be3fcc5116e00c31b90e45b, https://git.kernel.org/stable/c/dfaa39b05a6cf34a16c525a2759ee6ab26b5fef6	O-LIN-LINU-190924/3397

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
			#PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] SMP PTI CPU: 33 PID: 16573 Comm: kworker/u97:799 Not tainted 6.8.7-cm4all1-hp+ #43 Hardware name: HP ProLiant DL380 Gen9/ProLiant DL380 Gen9, BIOS P89 10/17/2018 Workqueue: events_unbound netfs_rreq_write_to_cache_work RIP: 0010:cachefiles_prepare_write+0x30/0xa0 Code: 57 41 56 45 89 ce 41 55 49 89 cd 41 54 49 89 d4 55 53 48 89 fb 48 83 ec 08 48 8b 47 08 48 83 7f 10 00 48 89 34 24 48 8b 68 20 <48> 8b 45 08 4c 8b 38 74 45 49 8b 7f 50 e8 4e a9 b0 ff 48 8b 73 10 RSP: 0018:ffffb4e78113		

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
			bde0 EFLAGS: 00010286 RAX: ffff976126be6d10 RBX: ffff97615cdb8438 RCX: 0000000000020000 RDX: ffff97605e6c4c68 RSI: ffff97605e6c4c60 RDI: ffff97615cdb8438 RBP: 0000000000000000 R08: 0000000000278333 R09: 0000000000000001 R10: ffff97605e6c4600 R11: 0000000000000001 R12: ffff97605e6c4c68 R13: 0000000000020000 R14: 0000000000000001 R15: ffff976064fe2c00 FS: 0000000000000000(0000) GS:ffff9776dfd40000(0000) knlGS:0000000000000000		

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
			CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000008 CR3: 000000005942c002 CR4: 00000000001706f0 Call Trace: <TASK> ? __die+0x1f/0x70 ? page_fault_oops+0x15d/0x440 ? search_module_extables+0xe/0x40 ? fixup_exception+0x22/0x2f0 ? exc_page_fault+0x5f/0x100 ? asm_exc_page_fault+0x22/0x30 ? cachefiles_prepare_write+0x30/0xa0 netfs_rreq_write_to_cache_work+0x135/0x2e0 process_one_work+0x137/0x2c0		

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
			worker_thread+0x2e9/0x400 ? __pfx_worker_thread+0x10/0x10 kthread+0xcc/0x100 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x30/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1b/0x30 </TASK> Modules linked in: CR2: 0000000000000008 ---[end trace 0000000000000000]--- This happened because fscache_cookie_state_machine() was slow and was still running while another process invoked		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			fscache_unuse_cookie();
			this led to a fscache_cookie_lru_do_one() call, setting the
			FSCACHE_COOKIE_DO_LRU_DISCARD flag, which was picked up by
			fscache_cookie_state_machine(), withdrawing the cookie via
			cachefiles_withdraw_cookie(), clearing cookie->cache_priv.
			
			At the same time, yet another process invoked
			cachefiles_prepare_write(), which found a NULL pointer in this code
			line:
			
			struct cachefiles_object *object = cachefiles_cres_object(cres);
			
			The next line crashes, obviously:
			
			struct cachefiles_cache		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			*cache = object->volume->cache; During cachefiles_prepare_write(), the "n_accesses" counter is non-zero (via fscache_begin_operation()). The cookie must not be withdrawn until it drops to zero. The counter is checked by fscache_cookie_state_machine() before switching to FSCACHE_COOKIE_STATE_RELINQUISHING and FSCACHE_COOKIE_STATE_WITHDRAWING (in "case FSCACHE_COOKIE_STATE_FAILED"), but not for FSCACHE_COOKIE_STATE_LRU_DISCARDING ("case FSCACHE_COOKIE_STATE_ACTIVE"). This patch adds the missing check. With a non-zero access counter,		

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 function returns and the next fscache_end_cookie_access() call will queue another fscache_cookie_state_machine() call to handle the still-pending FSCACHE_COOKIE_DO_LRU_DISCARD. **CVE ID: CVE-2024-45000**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: rtla/osnoise: Prevent NULL dereference in error handling If the "tool->data" allocation fails then there is no need to call osnoise_free_top() and, in fact, doing so will lead to a NULL dereference. **CVE ID: CVE-2024-45002**	https://git.kernel.org/stable/c/753f1745146e03abd17eec8eee95faffc96d743d, https://git.kernel.org/stable/c/90574d2a675947858b47008df8d07f75ea50d0d0, https://git.kernel.org/stable/c/abdb9ddaaab476e62805e36cce7b4ef8413ffd01	O-LIN-LINU-190924/3398
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/0f0654318e25b2c185e245ba4a591e42fabb5e59,	O-LIN-LINU-190924/3399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			xhci: Fix Panther point NULL pointer deref at full-speed re-enumeration re-enumerating full-speed devices after a failed address device command can trigger a NULL pointer dereference. Full-speed devices may need to reconfigure the endpoint 0 Max Packet Size value during enumeration. Usb core calls usb_ep0_reinit() in this case, which ends up calling xhci_configure_endpoint(). On Panther point xHC the xhci_configure_endpoint() function will additionally check and reserve bandwidth in software. Other hosts do this in hardware	https://git.kernel.org/stable/c/365ef7c4277fdd781a695c3553fa157d622d805d, https://git.kernel.org/stable/c/5ad898ae82412f8a689d59829804bff2999dd0ea	

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
			If xHC address device command fails then a new xhci_virt_device structure is allocated as part of re-enabling the slot, but the bandwidth table pointers are not set up properly here. This triggers the NULL pointer dereference the next time usb_ep0_reinit() is called and xhci_configure_endpoint() tries to check and reserve bandwidth [46710.713538] usb 3-1: new full-speed USB device number 5 using xhci_hcd [46710.713699] usb 3-1: Device not responding to setup address. [46710.917684] usb 3-1: Device not responding to setup address. [46711.125536] usb 3-1: device not accepting address 5, error -71		

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
			[46711.125594] BUG: kernel NULL pointer dereference, address: 0000000000000008 [46711.125600] #PF: supervisor read access in kernel mode [46711.125603] #PF: error_code(0x0000) - not-present page [46711.125606] PGD 0 P4D 0 [46711.125610] Oops: Oops: 0000 [#1] PREEMPT SMP PTI [46711.125615] CPU: 1 PID: 25760 Comm: kworker/1:2 Not tainted 6.10.3_2 #1 [46711.125620] Hardware name: Gigabyte Technology Co., Ltd. [46711.125623] Workqueue: usb_hub_wq hub_event [usbcore] [46711.125668] RIP: 0010:xhci_reserve_bandwidth		

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
			(drivers/usb/host/xhci.c Fix this by making sure bandwidth table pointers are set up correctly after a failed address device command, and additionally by avoiding checking for bandwidth in cases like this where no actual endpoints are added or removed, i.e. only context for default control endpoint 0 is evaluated. **CVE ID: CVE-2024-45006**		
N/A	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: only decrement add_addr_accepted for MPJ req Adding the following warning ...	https://git.kernel.org/stable/c/1c1f721375989579e46741f59523e39ec9b2a9bd, https://git.kernel.org/stable/c/2060f1efab370b496c4903b840844ecaff324c3c, https://git.kernel.org/stable/c/35b31f5549ede4070566b9497	O-LIN-LINU-190924/3400

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
			WARN_ON_ONCE(msk->pm.add_addr_accepted == 0) ... before decrementing the add_addr_accepted counter helped to find a bug when running the "remove single subflow" subtest from the mptcp_join.sh selftest. Removing a 'subflow' endpoint will first trigger a RM_ADDR, then the subflow closure. Before this patch, and upon the reception of the RM_ADDR, the other peer will then try to decrement this add_addr_accepted. That's not correct because the attached subflows have not been created upon the reception of an ADD_ADDR.	81e83495906b43d	

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
			A way to solve that is to decrement the counter only if the attached subflow was an MP_JOIN to a remote id that was not 0, and initiated by the host receiving the RM_ADDR. **CVE ID: CVE-2024-45009**		
N/A	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: only mark 'subflow' endp as available Adding the following warning ... WARN_ON_ONCE(msk->pm.local_addr_used == 0) ... before decrementing the local_addr_used counter helped to find a bug when running the "remove single address" subtest	https://git.kernel.org/stable/c/322ea3778965da72862cca2a0c50253aacf65fe6, https://git.kernel.org/stable/c/43cf912b0b0fc7b4fd12cbc735d1f5afb8e1322d, https://git.kernel.org/stable/c/7fdc870d08960961408a44c569f20f50940e7d4f	O-LIN-LINU-190924/3401

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
			from the mptcp_join.sh selftests. Removing a 'signal' endpoint will trigger the removal of all subflows linked to this endpoint via mptcp_pm_nl_rm_addr_or_subflow() with rm_type == MPTCP_MIB_RMSUBFLOW. This will decrement the local_addr_used counter, which is wrong in this case because this counter is linked to 'subflow' endpoints, and here it is a 'signal' endpoint that is being removed. Now, the counter is decremented, only if the ID is being used outside of mptcp_pm_nl_rm_addr_or_subflow(), only for 'subflow' endpoints, and if the ID is not 0 -- local_addr_used is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not taking into account these ones. This marking of the ID as being available, and the decrement is done no matter if a subflow using this ID is currently available, because the subflow could have been closed before. **CVE ID: CVE-2024-45010**		
N/A	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: char: xillybus: Check USB endpoints when probing device Ensure, as the driver probes the device, that all endpoints that the driver may attempt to access exist and are of the correct type. All XillyUSB devices must have a Bulk IN and Bulk OUT endpoint at address 1. This is verified in	https://git.kernel.org/stable/c/1371d32b95972d39c1e6e4bae8b6d0df1b573731, https://git.kernel.org/stable/c/2374bf7558de915edc6ec8cb10ec3291dfab9594, https://git.kernel.org/stable/c/25ee8b2908200fc862c0434e5ad483817d50ceda	O-LIN-LINU-190924/3402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			xillyusb_setup_base_eps(). On top of that, a XillyUSB device may have additional Bulk OUT endpoints. The information about these endpoints' addresses is deduced from a data structure (the IDT) that the driver fetches from the device while probing it. These endpoints are checked in setup_channels(). A XillyUSB device never has more than one IN endpoint, as all data towards the host is multiplexed in this single Bulk IN endpoint. This is why setup_channels() only checks OUT endpoints. **CVE ID: CVE-2024-45011**		
Allocation of Resources	11-Sep-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/57ca481fca97ca	O-LIN-LINU-190924/3403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Without Limits or Throttling			vulnerability has been resolved: nouveau/firmware: use dma non-coherent allocator Currently, enabling SG_DEBUG in the kernel will cause nouveau to hit a BUG() on startup, when the iommu is enabled: kernel BUG at include/linux/scatterlist.h:187! invalid opcode: 0000 [#1] PREEMPT SMP NOPTI CPU: 7 PID: 930 Comm: (udev-worker) Not tainted 6.9.0-rc3Lyude-Test+ #30 Hardware name: MSI MS-7A39/A320M GAMING PRO (MS-7A39), BIOS 1.I0 01/22/2019 RIP: 0010:sg_init_one+0x85/0xa0 Code: 69 88 32 01 83 e1 03 f6 c3 03 75	4553e8c85d6a94baf4cb40c40e, https://git.kernel.org/stable/c/9b340aeb26d50e9a9ec99599e2a39b035fac978e, https://git.kernel.org/stable/c/cc29c5546c6a373648363ac49781f1d74b530707	

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
			20 a8 01 75 1e 48 09 cb 41 89 54 24 08 49 89 1c 24 41 89 6c 24 0c 5b 5d 41 5c e9 7b b9 88 00 <0f> 0b 0f 0b 0f 0b 48 8b 05 5e 46 9a 01 eb b2 66 66 2e 0f 1f 84 00 RSP: 0018:ffffa776017bf6a0 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffffa77600d87000 RCX: 000000000000002b RDX: 0000000000000001 RSI: 0000000000000000 RDI: ffffa77680d87000 RBP: 000000000000e000 R08: 0000000000000000 R09: 0000000000000000 R10: ffff98f4c46aa508 R11: 0000000000000000 R12: ffff98f4c46aa508 R13: ffff98f4c46aa008		

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
			R14: ffffa77600d4a000 R15: ffffa77600d4a018 FS: 00007feeb5aae980 (0000) GS:ffff98f5c4dc0000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f22cb9a4520 CR3: 00000001043ba000 CR4: 00000000003506f0 Call Trace: <TASK> ? die+0x36/0x90 ? do_trap+0xdd/0x100 ? sg_init_one+0x85/0xa0 ? do_error_trap+0x65/0x80 ? sg_init_one+0x85/0xa0 ? exc_invalid_op+0x50/0x70		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? sg_init_one+0x85/0xa0 ? asm_exc_invalid_op+0x1a/0x20 ? sg_init_one+0x85/0xa0 nvkm_firmware_ctor+0x14a/0x250 [nouveau] nvkm_falcon_fw_ctor+0x42/0x70 [nouveau] ga102_gsp_booter_ctor+0xb4/0x1a0 [nouveau] r535_gsp_oneinit+0xb3/0x15f0 [nouveau] ? srso_return_thunk+0x5/0x5f ? srso_return_thunk+0x5/0x5f ? nvkm_udevice_new+0x95/0x140 [nouveau] ? srso_return_thunk+0x5/0x5f		

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
			? srso_return_thunk+0x5/0x5f ? ktime_get+0x47/0xb0 Fix this by using the non-coherent allocator instead, I think there might be a better answer to this, but it involve ripping up some of APIs using sg lists. **CVE ID: CVE-2024-45012**		
Use After Free	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netem: fix return value if duplicate enqueue fails There is a bug in netem_enqueue() introduced by commit 5845f706388a ("net: netem: fix skb length BUG_ON in __skb_to_sgvec") that can lead to a use-after-free.	https://git.kernel.org/stable/c/0486d31dd8198e22b63a4730244b38fffce6d469, https://git.kernel.org/stable/c/52d99a69f3d556c6426048c9d481b912205919d8, https://git.kernel.org/stable/c/577d6c0619467fe90f7e8e57e45cb5bd9d36014	O-LIN-LINU-190924/3404

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
			This commit made netem_enqueue() always return NET_XMIT_SUCCESS when a packet is duplicated, which can cause the parent qdisc's q.qlen to be mistakenly incremented. When this happens qlen_notify() may be skipped on the parent during destruction, leaving a dangling pointer for some classful qdiscs like DRR. There are two ways for the bug happen: - If the duplicated packet is dropped by rootq->enqueue() and then the original packet is also dropped. - If rootq->enqueue() sends the duplicated packet to a different qdisc and the original packet is dropped.		

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
			In both cases NET_XMIT_SUCCESS is returned even though no packets are enqueued at the netem qdisc. The fix is to defer the enqueue of the duplicate packet until after the original packet has been guaranteed to return NET_XMIT_SUCCESS. **CVE ID: CVE-2024-45016**		
Improper Initialization	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: initialise extack before use Fix missing initialisation of extack in flow offload. **CVE ID: CVE-2024-45018**	https://git.kernel.org/stable/c/119be227bc04f5035efa64cb823b8a5ca5e2d1c1, https://git.kernel.org/stable/c/356beb911b63a8cff34cb57f755c2a2d2ee9dec7, https://git.kernel.org/stable/c/7eafeec6be68ebd6140a830ce9ae68ad5b67ec78	O-LIN-LINU-190924/3405
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/046667c4d3196938e992fba0dfcde570aa85cd0e,	O-LIN-LINU-190924/3406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memcg_write_event_control(): fix a user-triggerable oops we are *not* guaranteed that anything past the terminating NUL is mapped (let alone initialized with anything sane). **CVE ID: CVE-2024-45021**	https://git.kernel.org/stable/c/0fbe2a72e853a1052abe9bc2b7df8ddb102da227, https://git.kernel.org/stable/c/1b37ec85ad95b612307627758c6018cd9d92cca8	
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fix bitmap corruption on close_range() with CLOSE_RANGE_UNSHARE copy_fd_bitmaps(new, old, count) is expected to copy the first count/BITS_PER_LONG bits from old->full_fds_bits[] and fill the rest with zeroes. What it does is copying enough words (BITS_TO_LONGS(count/BITS_PER_LO	https://git.kernel.org/stable/c/5053581fe5dfb09b58c65dd8462bf5dea71f41ff, https://git.kernel.org/stable/c/8cad3b2b3ab81ca55f37405ffd1315bcc2948058, https://git.kernel.org/stable/c/9a2fa1472083580b6c66bdaf291f591e1170123a	O-LIN-LINU-190924/3407

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
			NG)), then memsets the rest. That works fine, *if* all bits past the cutoff point are clear. Otherwise we are risking garbage from the last word we'd copied. For most of the callers that is true - expand_fdtable() has count equal to old->max_fds, so there's no open descriptors past count, let alone fully occupied words in ->open_fds[], which is what bits in ->full_fds_bits[] correspond to. The other caller (dup_fd()) passes sane_fdtable_size(old_fdt, max_fds), which is the smallest multiple of BITS_PER_LONG that covers all opened descriptors below max_fds. In the common case (copying on		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fork()) max_fds is ~0U, so all opened descriptors will be below it and we are fine, by the same reasons why the call in expand_fdtable() is safe. Unfortunately, there is a case where max_fds is less than that and where we might, indeed, end up with junk in ->full_fds_bits[] - close_range(from, to, CLOSE_RANGE_UNSHARE) with * descriptor table being currently shared * 'to' being above the current capacity of descriptor table * 'from' being just under some chunk of opened descriptors. In that case we end up with observably wrong behaviour - e.g. spawn		

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
			a child with CLONE_FILES, get all descriptors in range 0..127 open, then close_range(64, ~0U, CLOSE_RANGE_UNSHARE) and watch dup(0) ending up with descriptor #128, despite #64 being observably not open. The minimally invasive fix would be to deal with that in dup_fd(). If this proves to add measurable overhead, we can go that way, but let's try to fix copy_fd_bitmaps() first. * new helper: bitmap_copy_and_expand(to, from, bits_to_copy, size). * make copy_fd_bitmaps() take the bitmap size in words, rather than bits; it's 'count' argument is always a multiple of BITS_PER_LONG,		

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
			so we are not losing any information, and that way we can use the same helper for all three bitmaps - compiler will see that count is a multiple of BITS_PER_LONG for the large ones, so it'll generate plain memcpy()+memset(). Reproducer added to tools/testing/selftests/core/close_range_test.c **CVE ID: CVE-2024-45025**		
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mmc: mmc_test: Fix NULL dereference on allocation failure If the "test->highmem = alloc_pages()" allocation fails then calling __free_pages(test->highmem) will	https://git.kernel.org/stable/c/2b507b03991f44dfb202fc2a82c9874d1b1f0c06, https://git.kernel.org/stable/c/3b4e76ceae5b5a46c968bd952f551ce173809f63, https://git.kernel.org/stable/c/9b9ba386d7bfdbc38445932c90fa9444c0524bea	O-LIN-LINU-190924/3408

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
			result in a NULL dereference. Also change the error code to -ENOMEM instead of returning success. **CVE ID: CVE-2024-45028**		
Improper Locking	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: i2c: tegra: Do not mark ACPI devices as irq safe On ACPI machines, the tegra i2c module encounters an issue due to a mutex being called inside a spinlock. This leads to the following bug: BUG: sleeping function called from invalid context at kernel/locking/mutex.c:585 ... Call trace: __might_sleep __mutex_lock_common	https://git.kernel.org/stable/c/14d069d92951a3e150c0a81f2ca3b93e54da913b, https://git.kernel.org/stable/c/2853e1376d8161b04c9ff18ba82b43f08a049905, https://git.kernel.org/stable/c/6861faf4232e4b78878f2de1ed3ee324ddae2287	O-LIN-LINU-190924/3409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mutex_lock_ nested acpi_subsys _runtime_resume rpm_resume tegra_i2c_xf er The problem arises because during __pm_runtime_resu me(), the spinlock &dev->power.lock is acquired before rpm_resume() is called. Later, rpm_resume() invokes acpi_subsys_runtim e_resume(), which relies on mutexes, triggering the error. To address this issue, devices on ACPI are now marked as not IRQ-safe, considering the dependency of acpi_subsys_runtim e_resume() on mutexes. **CVE ID: CVE-2024-45029**		
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.49					
Double Free	13-Sep-2024	7.8	In the Linux kernel, the following	https://git.kern el.org/stable/c/	O-LIN-LINU-190924/3410

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
			vulnerability has been resolved: scsi: aacraid: Fix double-free on probe failure aac_probe_one() calls hardware-specific init functions through the aac_driver_ident::init pointer, all of which eventually call down to aac_init_adapter(). If aac_init_adapter() fails after allocating memory for aac_dev::queues, it frees the memory but does not clear that member. After the hardware-specific init function returns an error, aac_probe_one() goes down an error path that frees the memory pointed to by aac_dev::queues, resulting.in a double-free.	4b540ec7c0045c2d01c4e479f34bbc8f147afa4c, https://git.kernel.org/stable/c/564e1986b00c5f05d75342f8407f75f0a17b94df, https://git.kernel.org/stable/c/60962c3d8e18e5d8dfa16df788974dd7f35bd87a	

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
			CVE ID: CVE-2024-46673		
Use After Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: dwc3: st: fix probed platform device ref count on probe error path The probe function never performs any paltform device allocation, thus error path "undo_platform_dev_alloc" is entirely bogus. It drops the reference count from the platform device being probed. If error path is triggered, this will lead to unbalanced device reference counts and premature release of device resources, thus possible use-after-free when releasing remaining devm-managed resources. **CVE ID: CVE-2024-46674**	https://git.kernel.org/stable/c/060f41243ad7f6f5249fa7290dda0c01f723d12d, https://git.kernel.org/stable/c/1de989668708ce5875efc9d669d227212aeb9a90, https://git.kernel.org/stable/c/4c6735299540f3c82a5033d35be76a5c42e0fb18	O-LIN-LINU-190924/3411

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
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: gtp: fix a potential NULL pointer dereference When sockfd_lookup() fails, gtp_encap_enable_socket() returns a NULL pointer, but its callers only check for error pointers thus miss the NULL pointer case. Fix it by returning an error pointer with the error code carried from sockfd_lookup(). (I found this bug during code inspection.) **CVE ID: CVE-2024-46677**	https://git.kernel.org/stable/c/28c67f0f84f889fe9f4cbda8354132b20dc9212d, https://git.kernel.org/stable/c/4643b91691e969b1b9ad54bf552d7a990cfa3b87, https://git.kernel.org/stable/c/612edd35f2a3910ab1f61c1f2338889d4ba99fa2	O-LIN-LINU-190924/3412
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: pinctrl: single: fix potential NULL	https://git.kernel.org/stable/c/0a2bab5ed161318f57134716accba0a30f3af191, https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dereference in pcs_get_function() pinmux_generic_get_function() can return NULL and the pointer 'function' was dereferenced without checking against NULL. Add checking of pointer 'function' in pcs_get_function(). Found by code review. **CVE ID: CVE-2024-46685**	1c38a62f15e595346a1106025722869e87ffe044, https://git.kernel.org/stable/c/292151af6add3e5ab11b2e9916cffa5f52859a1f	
Affected Version(s): From (including) 6.3 Up to (excluding) 6.6.48					
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/vmalloc: fix page mapping if vm_area_alloc_pages() with high order fallback to order 0 The __vmap_pages_range_noflush() assumes its argument pages** contains pages with the same page shift.	https://git.kernel.org/stable/c/61ebe5a747da649057c37be1c37eb934b4af79ca, https://git.kernel.org/stable/c/c91618816f4d21fc574d7577a37722adcd4075b2, https://git.kernel.org/stable/c/de7bad86345c43cd040ed43e20d9fad78a3ee59f	O-LIN-LINU-190924/3414

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
			However, since commit e9c3cda4d86e ("mm, vmalloc: fix high order __GFP_NOFAIL allocations"), if gfp_flags includes __GFP_NOFAIL with high order in vm_area_alloc_pages() and page allocation failed for high order, the pages** may contain two different page shifts (high order and order-0). This could lead __vmap_pages_range_noflush() to perform incorrect mappings, potentially resulting in memory corruption. Users might encounter this as follows (vmap_allow_huge = true, 2M is for PMD_SIZE):		

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
			kvmalloc(2M, __GFP_NOFAIL|GFP_X) __vmalloc_node_range_noprof(vm_flags=VM_ALLOW_HUGE_VMAP) vm_area_alloc_pages(order=9) ---> order-9 allocation failed and fallback to order-0 vmap_pages_range() vmap_pages_range_noflush() __vmap_pages_range_noflush(page_shift = 21) ----> wrong mapping happens We can remove the fallback code because if a high-order allocation fails, __vmalloc_node_range_noprof() will retry with order-0. Therefore, it is unnecessary to fallback to order-0 here. Therefore, fix this by removing the fallback code.		

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
			CVE ID: CVE-2024-45022		
Affected Version(s): From (including) 6.3 Up to (excluding) 6.6.49					
Double Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix a use-after-free when hitting errors inside btrfs_submit_chunk() [BUG] There is an internal report that KASAN is reporting use-after-free, with the following backtrace: BUG: KASAN: slab-use-after-free in btrfs_check_read_bio+0xa68/0xb70 [btrfs] Read of size 4 at addr ffff8881117cec28 by task kworker/u16:2/45 CPU: 1 UID: 0 PID: 45 Comm: kworker/u16:2 Not tainted 6.11.0-rc2-next-20240805-default+ #76	https://git.kernel.org/stable/c/10d9d8c3512f16cad47b2ff81ec6fc4b27d8ee10, https://git.kernel.org/stable/c/4a3b9e1a8e6cd1a8d427a905e159de58d38941cc, https://git.kernel.org/stable/c/51722b99f41f5e722ffa10b8f61e802a0e70b331	O-LIN-LINU-190924/3415

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
			Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.2-3-gd478f380-rebuilt.opensuse.org 04/01/2014 Workqueue: btrfs-endio btrfs_end_bio_work [btrfs] Call Trace: dump_stack_lvl+0x61/0x80 print_address_description.constprop.0+0x5e/0x2f0 print_report+0x118/0x216 kasan_report+0x11d/0x1f0 btrfs_check_read_bio+0xa68/0xb70 [btrfs] process_one_work+0xce0/0x12a0 worker_thread+0x717/0x1250 kthread+0x2e3/0x3c0		

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
			ret_from_fork+0x2d/0x70 ret_from_fork_asm+0x11/0x20 Allocated by task 20917: kasan_save_stack+0x37/0x60 kasan_save_track+0x10/0x30 __kasan_slab_alloc+0x7d/0x80 kmem_cache_alloc_noprof+0x16e/0x3e0 mempool_alloc_noprof+0x12e/0x310 bio_alloc_bioset+0x3f0/0x7a0 btrfs_bio_alloc+0x2e/0x50 [btrfs] submit_extent_page+0x4d1/0xdb0 [btrfs] btrfs_do_readpage+0x8b4/0x12a0 [btrfs]		

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
			btrfs_readahead+0x29a/0x430 [btrfs] read_pages+0x1a7/0xc60 page_cache_ra_unbounded+0x2ad/0x560 filemap_get_pages+0x629/0xa20 filemap_read+0x335/0xbf0 vfs_read+0x790/0xcb0 ksys_read+0xfd/0x1d0 do_syscall_64+0x6d/0x140 entry_SYSCALL_64_after_hwframe+0x4b/0x53 Freed by task 20917: kasan_save_stack+0x37/0x60 kasan_save_track+0x10/0x30		

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
			kasan_save_free_info+0x37/0x50 __kasan_slab_free+0x4b/0x60 kmem_cache_free+0x214/0x5d0 bio_free+0xed/0x180 end_bbio_data_read+0x1cc/0x580 [btrfs] btrfs_submit_chunk+0x98d/0x1880 [btrfs] btrfs_submit_bio+0x33/0x70 [btrfs] submit_one_bio+0xd4/0x130 [btrfs] submit_extent_page+0x3ea/0xdb0 [btrfs] btrfs_do_readpage+0x8b4/0x12a0 [btrfs] btrfs_readahead+0x29a/0x430 [btrfs] read_pages+0x1a7/0xc60		

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
			page_cache_ra_unbounded+0x2ad/0x560 filemap_get_pages+0x629/0xa20 filemap_read+0x335/0xbf0 vfs_read+0x790/0xcb0 ksys_read+0xfd/0x1d0 do_syscall_64+0x6d/0x140 entry_SYSCALL_64_after_hwframe+0x4b/0x53 [CAUSE] Although I cannot reproduce the error, the report itself is good enough to pin down the cause. The call trace is the regular endio workqueue context, but the free-by-task trace is showing that during		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			btrfs_submit_chunk () we already hit a critical error, and is calling btrfs_bio_end_io() to error out. And the original endio function called bio_put() to free the whole bio. This means a double freeing thus causing use-after-free, e.g.: 1. Enter btrfs_submit_bio() with a read bio The read bio length is 128K, crossing two 64K stripes. 2. The first run of btrfs_submit_chunk () 2.1 Call btrfs_map_block(), which returns 64K 2.2 Call btrfs_split_bio() Now there are two bios, one referring to the first 64K, the other		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			referring to the second 64K. 2.3 The first half is submitted. 3. The second run of btrfs_submit_chunk () 3.1 Call btrfs_map_block(), which by somehow failed Now we call btrfs_bio_end_io() to handle the error 3.2 btrfs_bio_end_io() calls the original endio function Which is end_bbio_data_rea d(), and it calls bio_put() for the original bio. Now the original bio is freed. 4. The submitted first 64K bio finished Now we call into btrfs_check_read_bi o() and tries to advance the bio		

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
			iter. But since the original bio (thus its iter) is already freed, we trigger the above use-after free. And even if the memory is not poisoned/corrupted, we will later call the original endio function, causing a double freeing. [FIX] Instead of calling btrfs_bio_end_io(), call btrfs_orig_bbio_end_io(), which has the extra check on split bios and do the pr ---truncated--- **CVE ID: CVE-2024-46687**		
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: smb/client: avoid dereferencing rdata=NULL in smb2_new_read_req()	https://git.kernel.org/stable/c/6df57c63c200cd05e085c3b695128260e21959b7, https://git.kernel.org/stable/c/a01859dd6aebf826576513850a3b05992809e9d2,	O-LIN-LINU-190924/3416

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
			This happens when called from SMB2_read() while using rdma and reaching the rdma_readwrite_threshold. **CVE ID: CVE-2024-46686**	https://git.kernel.org/stable/c/b902fb78ab21299e4dd1775e7e8d251d5c0735bc	
Improper Locking	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: firmware: qcom: scm: Mark get_wq_ctx() as atomic call Currently get_wq_ctx() is wrongly configured as a standard call. When two SMC calls are in sleep and one SMC wakes up, it calls get_wq_ctx() to resume the corresponding sleeping thread. But if get_wq_ctx() is interrupted, goes to sleep and another SMC call is waiting to be allocated a waitq context, it leads to a deadlock.	https://git.kernel.org/stable/c/9960085a3a82c58d3323c1c20b991db6045063b0, https://git.kernel.org/stable/c/cdf7efe4b02aa93813db0bf1ca596ad298ab6b06, https://git.kernel.org/stable/c/e40115c33c0d79c940545b6b12112aace7acd9f5	O-LIN-LINU-190924/3417

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
			To avoid this get_wq_ctx() must be an atomic call and can't be a standard SMC call. Hence mark get_wq_ctx() as a fast call. **CVE ID: CVE-2024-46692**		
NULL Pointer Dereference	13-Sep-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: soc: qcom: pmic_glink: Fix race during initialization As pointed out by Stephen Boyd it is possible that during initialization of the pmic_glink child drivers, the protection-domain notifiers fires, and the associated work is scheduled, before the client registration returns and as a result the local "client" pointer has been initialized. The outcome of this is a NULL pointer	https://git.kernel.org/stable/c/1efdbf5323c9360e05066049b97414405e94e087, https://git.kernel.org/stable/c/3568affcddd68743e25aa3ec1647d9b82797757b, https://git.kernel.org/stable/c/943b0e7cc646a624bb20a68080f8f1a4a55df41c	O-LIN-LINU-190924/3418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dereference as the "client" pointer is blindly dereferenced. Timeline provided by Stephen: CPU0 CPU1 ---- ---- ucsi->client = NULL; devm_pmic_glink_register_client() client->pdr_notify(client->priv, pg->client_state) pmic_glink_ucsi_pdr_notify() schedule_work(&ucsi->register_work) <schedule away> pmic_glink_ucsi_register() ucsi_register() pmic_glink_ucsi_read_version() pmic_glink_ucsi_read()		

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
			pmic_glink_ucsi_read() pmic_glink_send(ucsi->client) <client is NULL BAD> ucsi->client = client // Too late! This code is identical across the altmode, battery manager and usci child drivers. Resolve this by splitting the allocation of the "client" object and the registration thereof into two operations. This only happens if the protection domain registry is populated at the time of registration, which by the introduction of commit '1ebcde047c54 ("soc: qcom: add pd-mapper implementation")'		

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
			became much more likely. **CVE ID: CVE-2024-46693**		
Affected Version(s): From (including) 6.4 Up to (excluding) 6.6.48					
Uncontrolled Recursion	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: vsock: fix recursive ->recvmsg calls After a vsock socket has been added to a BPF sockmap, its prot->recvmsg has been replaced with vsock_bpf_recvmsg(). Thus the following recursiion could happen: vsock_bpf_recvmsg() -> __vsock_recvmsg() -> vsock_connectible_recvmsg() -> prot->recvmsg() -> vsock_bpf_recvmsg() again	https://git.kernel.org/stable/c/69139d2919dd4aa9a553c8245e7c63e82613e3fc, https://git.kernel.org/stable/c/921f1acf0c3cf6b1260ab57a8a6e8b3d5f3023d5, https://git.kernel.org/stable/c/b4ee8cf1acc5018ed1369150d7bb3e0d0f79e135	O-LIN-LINU-190924/3419

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
			We need to fix it by calling the original ->recvmsg() without any BPF sockmap logic in __vsock_recvmsg(). **CVE ID: CVE-2024-44996**		
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: igb: cope with large MAX_SKB_FRAGS Sabrina reports that the igb driver does not cope well with large MAX_SKB_FRAG values: setting MAX_SKB_FRAG to 45 causes payload corruption on TX. An easy reproducer is to run ssh to connect to the machine. With MAX_SKB_FRAGS=17 it works, with MAX_SKB_FRAGS=45 it fails. This has been reported originally in https://bugzilla.redhat.com/show_bug.cgi?id=2265320	https://git.kernel.org/stable/c/8aba27c4a5020abdf60149239198297f88338a8d, https://git.kernel.org/stable/c/8ea80ff5d8298356d28077bc30913ed37df65109, https://git.kernel.org/stable/c/b52bd8bcb9e8ff250c79b44f9af8b15cae8911ab	O-LIN-LINU-190924/3420

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 root cause of the issue is that the driver does not take into account properly the (possibly large) shared info size when selecting the ring layout, and will try to fit two packets inside the same 4K page even when the 1st fraglist will trump over the 2nd head. Address the issue by checking if 2K buffers are insufficient. **CVE ID: CVE-2024-45030**		
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: cfg80211: Handle SSID based pmksa deletion wpa_supplicant 2.11 sends since 1efdba5fdc2c ("Handle PMKSA flush in the	https://git.kernel.org/stable/c/1f566eb912d192c83475a919331aea59619e1197, https://git.kernel.org/stable/c/2ad4e1ada8eebafa2d75a4b75eeeca882de6ada1, https://git.kernel.org/stable/c/4291f94f8c6b01505132c22ee2	O-LIN-LINU-190924/3421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			driver for SAE/OWE offload cases") SSID based PMKSA del commands. brcmfmac is not prepared and tries to dereference the NULL bssid and pmkid pointers in cfg80211_pmksa. PMKID_V3 operations support SSID based updates so copy the SSID. **CVE ID: CVE-2024-46672**	7b59ed27c3584f	
Affected Version(s): From (including) 6.5 Up to (excluding) 6.10.8					
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: video/aperture: optionally match the device in sysfb_disable() In aperture_remove_conflicting_pci_devices(), we currently only call sysfb_disable() on vga class devices. This leads to the following problem when the pimary	https://git.kernel.org/stable/c/17e78f43de0c6da34204cc858b4cc05671ea9acf, https://git.kernel.org/stable/c/b49420d6a1aeb399e5b107fc6eb8584d0860fbd7	O-LIN-LINU-190924/3422

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
			device is not VGA compatible: 1. A PCI device with a non-VGA class is the boot display 2. That device is probed first and it is not a VGA device so sysfb_disable() is not called, but the device resources are freed by aperture_detach_platform_device() 3. Non-primary GPU has a VGA class and it ends up calling sysfb_disable() 4. NULL pointer dereference via sysfb_disable() since the resources have already been freed by aperture_detach_platform_device() when it was called by the other device. Fix this by passing a device pointer to sysfb_disable() and checking the device to determine if we		

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
			should execute it or not. v2: Fix build when CONFIG_SCREEN_INFO is not set v3: Move device check into the mutex Drop primary variable in aperture_remove_conflicting_pci_devices() Drop __init on pci sysfb_pci_dev_is_enabled() **CVE ID: CVE-2024-46698**		
Affected Version(s): From (including) 6.6.15 Up to (excluding) 6.6.48					
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix a kernel verifier crash in stacksafe() Daniel Hodges reported a kernel verifier crash when playing with sched-ext. Further investigation shows that the crash is due to	https://git.kernel.org/stable/c/6e3987ac310c74bb4dd6a2fa8e46702fe505fb2b, https://git.kernel.org/stable/c/7cad3174cc79519bf5f6c4441780264416822c08, https://git.kernel.org/stable/c/bed2eb964c70b780fb55925892a74f26cb590b25	O-LIN-LINU-190924/3423

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
			invalid memory access in stacksafe(). More specifically, it is the following code: if (exact != NOT_EXACT && old->stack[spi].slot_type[i % BPF_REG_SIZE] != cur->stack[spi].slot_type[i % BPF_REG_SIZE]) return false; The 'i' iterates old->allocated_stack. If cur->allocated_stack < old->allocated_stack the out-of-bound access will happen. To fix the issue add 'i >= cur->allocated_stack' check such that if the condition is true, stacksafe() should fail. Otherwise, cur->stack[spi].slot_type[i % BPF_REG_SIZE]		

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
			memory access is legal. **CVE ID: CVE-2024-45020**		
Affected Version(s): From (including) 6.6.35 Up to (excluding) 6.6.46					
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: driver core: Fix uevent_show() vs driver detach race uevent_show() wants to de-reference dev->driver->name. There is no clean way for a device attribute to de-reference dev->driver unless that attribute is defined via (struct device_driver).dev_groups. Instead, the anti-pattern of taking the device_lock() in the attribute handler risks deadlocks with code paths that remove device attributes while holding the lock.	https://git.kernel.org/stable/c/15fffc6a5624b13b428bb1c6e9088e32a55eb82c, https://git.kernel.org/stable/c/49ea4e0d862632d51667da5e7a9c88a560e9c5a1, https://git.kernel.org/stable/c/4a7c2a8387524942171037e70b80e969c3b5c05b	O-LIN-LINU-190924/3424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This deadlock is typically invisible to lockdep given the device_lock() is marked lockdep_set_novalidate_class(), but some subsystems allocate a local lockdep key for @dev->mutex to reveal reports of the form: ========== ========== ========== ========= WARNING: possible circular locking dependency detected 6.10.0-rc7+ #275 Tainted: G OE N --- --- --- modprobe/2374 is trying to acquire lock: ffff8c2270070de0 (kn->active#6){++++}-{0:0}, at: __kernfs_remove+0xde/0x220		

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
			but task is already holding lock: ffff8c22016e88f8 (&cxl_root_key){+.+.}-{3:3}, at: device_release_driver_internal+0x39/0x210 which lock already depends on the new lock. the existing dependency chain (in reverse order) is: -> #1 (&cxl_root_key){+.+.}-{3:3}: __mutex_lock+0x99/0xc30 uevent_show+0xac/0x130 dev_attr_show+0x18/0x40 sysfs_kf_seq_show+0xac/0xf0 seq_read_iter+0x110/0x450 vfs_read+0x25b/0x340		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ksys_read+0x67/0xf0 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e -> #0 (kn->active#6){++++}-{0:0}: __lock_acquire+0x121a/0x1fa0 lock_acquire+0xd6/0x2e0 kernfs_drain+0x1e9/0x200 __kernfs_remove+0xde/0x220 kernfs_remove_by_name_ns+0x5e/0xa0 device_del+0x168/0x410 device_unregister+0x13/0x60 devres_release_all+0xb8/0x110		

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
			device_unbind_cleanup+0xe/0x70 device_release_driver_internal+0x1c7/0x210 driver_detach+0x47/0x90 bus_remove_driver+0x6c/0xf0 cxl_acpi_exit+0xc/0x11 [cxl_acpi] __do_sys_delete_module.isra.0+0x181/0x260 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e The observation though is that driver objects are typically much longer lived than device objects. It is reasonable to perform lockless de-reference of a @driver pointer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			even if it is racing detach from a device. Given the infrequency of driver unregistration, use synchronize_rcu() in module_remove_driver() to close any potential races. It is potentially overkill to suffer synchronize_rcu() just to handle the rare module removal racing uevent_show() event. Thanks to Tetsuo Handa for the debug analysis of the syzbot report [1]. **CVE ID: CVE-2024-44952**		
Affected Version(s): From (including) 6.6.8 Up to (excluding) 6.6.48					
Improper Locking	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Take state lock during tx timeout reporter	https://git.kernel.org/stable/c/03d3734bd692affe4d0e9c9d638f491aaf37411b, https://git.kernel.org/stable/c/8e57e66ecbdd2fddc9fbf3e984b1c523b70e9809	O-LIN-LINU-190924/3425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mlx5e_safe_reopen _channels() requires the state lock taken. The referenced changed in the Fixes tag removed the lock to fix another issue. This patch adds it back but at a later point (when calling mlx5e_safe_reopen _channels()) to avoid the deadlock referenced in the Fixes tag. **CVE ID: CVE-2024-45019**	, https://git.kernel.org/stable/c/b3b9a87adee97854bcd71057901d46943076267e	
Affected Version(s): From (including) 6.7 Up to (excluding) 6.10.5					
Missing Release of Memory after Effective Lifetime	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: idpf: fix memory leaks and crashes while performing a soft reset The second tagged commit introduced a UAF, as it removed restoring q_vector->vport pointers after reinitializating the structures. This is due to that all queue allocation	https://git.kernel.org/stable/c/6b289f8d91537ec1e4f9c7b38b31b90d93b1419b, https://git.kernel.org/stable/c/f01032a2ca099ec8d619aaa916c3762aa62495df	O-LIN-LINU-190924/3426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functions are performed here with the new temporary vport structure and those functions rewrite the backpointers to the vport. Then, this new struct is freed and the pointers start leading to nowhere. But generally speaking, the current logic is very fragile. It claims to be more reliable when the system is low on memory, but in fact, it consumes two times more memory as at the moment of running this function, there are two vports allocated with their queues and vectors. Moreover, it claims to prevent the driver from running into "bad state", but in fact, any error during the rebuild leaves the old vport in the		

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
			partially allocated state. Finally, if the interface is down when the function is called, it always allocates a new queue set, but when the user decides to enable the interface later on, vport_open() allocates them once again, IOW there's a clear memory leak here. Just don't allocate a new queue set when performing a reset, that solves crashes and memory leaks. Readd the old queue number and reopen the interface on rollback - that solves limbo states when the device is left disabled and/or without HW queues enabled. **CVE ID: CVE-2024-44964**		
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/1c682593096a	O-LIN-LINU-190924/3427

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
			vulnerability has been resolved: xen: privcmd: Switch from mutex to spinlock for irqfds irqfd_wakeup() gets EPOLLHUP, when it is called by eventfd_release() by way of wake_up_poll(&ctx->wqh, EPOLLHUP), which gets called under spin_lock_irqsave(). We can't use a mutex here as it will lead to a deadlock. Fix it by switching over to a spin lock. **CVE ID: CVE-2024-44957**	487fd9aebc079a307ff7a6d054a3, https://git.kernel.org/stable/c/49f2a5da6785b2dbde93e291cae037662440346e, https://git.kernel.org/stable/c/c2775ae4d9227729f8ca9ee2a068f62a00d5ea9c	
Missing Release of Memory after Effective Lifetime	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: dsa: bcm_sf2: Fix a possible memory leak in bcm_sf2_mdio_register()	https://git.kernel.org/stable/c/7feef10768ea71d468d9bbc1e0d14c461876768c, https://git.kernel.org/stable/c/a7d2808d67570e6acae45c2a96e0d59986888e4c, https://git.kern	O-LIN-LINU-190924/3428

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
			bcm_sf2_mdio_register() calls of_phy_find_device() and then phy_device_remove() in a loop to remove existing PHY devices. of_phy_find_device() eventually calls bus_find_device(), which calls get_device() on the returned struct device * to increment the refcount. The current implementation does not decrement the refcount, which causes memory leak. This commit adds the missing phy_device_free() call to decrement the refcount via put_device() to balance the refcount. **CVE ID: CVE-2024-44971**	el.org/stable/c/b7b8d9f5e679af60c94251fd6728dde34be69a71	
Affected Version(s): From (including) 6.7 Up to (excluding) 6.10.7					
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/09e086a5f72ea27c758b3f3b41	O-LIN-LINU-190924/3429

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
			atm: idt77252: prevent use after free in dequeue_rx() We can't dereference "skb" after calling vcc->push() because the skb is released. **CVE ID: CVE-2024-44998**	9a69000c32adc1, https://git.kernel.org/stable/c/1cece837e387c039225f19028df255df87a97c0d, https://git.kernel.org/stable/c/24cf390a5426aac9255205e9533cdd7b4235d518	
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: avoid possible UaF when selecting endp select_local_address() and select_signal_address() both select an endpoint entry from the list inside an RCU protected section, but return a reference to it, to be read later on. If the entry is dereferenced after the RCU unlock, reading info could cause a Use-after-Free. A simple solution is to copy the	https://git.kernel.org/stable/c/0201d65d9806d287a00e0ba96f0321835631f63f, https://git.kernel.org/stable/c/48e50dcbcbaaf713d82bf2da5c16aeced94ad07d, https://git.kernel.org/stable/c/9a9afbbc3fbfca4975eea4aa5b18556db5a0c0b8	O-LIN-LINU-190924/3430

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
			required info while inside the RCU protected section to avoid any risk of UaF later. The address ID might need to be modified later to handle the ID0 case later, so a copy seems OK to deal with. **CVE ID: CVE-2024-44974**		
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent possible UAF in ip6_xmit() If skb_expand_head() returns NULL, skb has been freed and the associated dst/idev could also have been freed. We must use rcu_read_lock() to prevent a possible UAF. **CVE ID: CVE-2024-44985**	https://git.kernel.org/stable/c/124b428fe28064c809e4237b0b38e97200a8a4a8, https://git.kernel.org/stable/c/2d5ff7e339d04622d8282661df36151906d0e1c7, https://git.kernel.org/stable/c/38a21c026ed2cc7232414cb166efc1923f34af17	O-LIN-LINU-190924/3431
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: ipv6: fix possible UAF in	https://git.kernel.org/stable/c/3574d28caf9a09756ae87ad1ea096c6f47b6101e, https://git.kern	O-LIN-LINU-190924/3432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ip6_finish_output2() If skb_expand_head() returns NULL, skb has been freed and associated dst/idev could also have been freed. We need to hold rcu_read_lock() to make sure the dst and associated idev are alive. **CVE ID: CVE-2024-44986**	el.org/stable/c/56efc253196751ece1fc535a5b582be127b0578a, https://git.kernel.org/stable/c/6ab6bf731354a6fdbaa617d1ec194960db61cf3b	
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent UAF in ip6_send_skb() syzbot reported an UAF in ip6_send_skb() [1] After ip6_local_out() has returned, we no longer can safely dereference rt, unless we hold rcu_read_lock().	https://git.kernel.org/stable/c/24e93695b1239fbe4c31e224372be77f82dab69a, https://git.kernel.org/stable/c/571567e0277008459750f0728f246086b2659429, https://git.kernel.org/stable/c/9a3e55afa95ed4ac9eda112d4f918af645d72f25	O-LIN-LINU-190924/3433

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
			A similar issue has been fixed in commit a688caa34beb ("ipv6: take rcu lock in rawv6_send_hdrinc()") Another potential issue in ip6_finish_output2() is handled in a separate patch. [1] BUG: KASAN: slab-use-after-free in ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 Read of size 8 at addr ffff88806dde4858 by task syz.1.380/6530 CPU: 1 UID: 0 PID: 6530 Comm: syz.1.380 Not tainted 6.11.0-rc3-syzkaller-00306-gdf6cbc62cc9b #0 Hardware name: Google Google Compute Engine/Google Compute Engine,		

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
			BIOS Google 08/06/2024 Call Trace: <TASK> __dump_stack lib/dump_stack.c:93 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:119 print_address_description mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x143/0x180 mm/kasan/report.c:601 ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 rawv6_push_pending_frames+0x75c/0x9e0 net/ipv6/raw.c:588 rawv6_sendmsg+0x19c7/0x23c0		

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
			net/ipv6/raw.c:926 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 sock_write_iter+0x2dd/0x400 net/socket.c:1160 do_iter_readv_writev+0x60a/0x890 vfs_writev+0x37c/0xbb0 fs/read_write.c:971 do_writev+0x1b1/0x350 fs/read_write.c:1018 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f		

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
			RIP: 0033:0x7f936bf79e79 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 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 a8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f936cd7f038 EFLAGS: 00000246 ORIG_RAX: 0000000000000014 RAX: ffffffffffffffda RBX: 00007f936c115f80 RCX: 00007f936bf79e79 RDX: 0000000000000001 RSI: 0000000020000040 RDI: 0000000000000004 RBP: 00007f936bfe7916 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11:		

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
			0000000000000246 R12: 0000000000000000 R13: 0000000000000000 R14: 00007f936c115f80 R15: 00007fff2860a7a8 </TASK> Allocated by task 6530: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 unpoison_slab_object mm/kasan/common.c:312 [inline] __kasan_slab_alloc+0x66/0x80 mm/kasan/common.c:338 kasan_slab_alloc include/linux/kasan.h:201 [inline] slab_post_alloc_hook mm/slub.c:3988 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_noprof+0x135/0x2a0 mm/slub.c:4044 dst_alloc+0x12b/0x190 net/core/dst.c:89 ip6_blackhole_route+0x59/0x340 net/ipv6/route.c:2670 make_blackhole net/xfrm/xfrm_policy.c:3120 [inline] xfrm_lookup_route+0xd1/0x1c0 net/xfrm/xfrm_policy.c:3313 ip6_dst_lookup_flow+0x13e/0x180 net/ipv6/ip6_output.c:1257 rawv6_sendmsg+0x1283/0x23c0 net/ipv6/raw.c:898 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+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
			x1a6/0x270 net/socket.c:745 ___sys_sendmsg+0x525/0x7d0 net/socket.c:2597 ___sys_sendmsg net/socket.c:2651 [inline] __sys_sendmsg+0x2b0/0x3a0 net/socket.c:2680 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 45: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 kasan_save_free_info+0x40/0x50 mm/kasan/generic.c:579		

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
			poison_slab_object +0xe0/0x150 mm/kasan/common.c:240 __kasan_slab_free+ 0x37/0x60 mm/kasan/common.c:256 kasan_slab_free include/linux/kasan.h:184 [inline] slab_free_hook mm/slub.c:2252 [inline] slab_free mm/slub.c:4473 [inline] kmem_cache_free+ 0x145/0x350 mm/slub.c:4548 dst_destroy+0x2ac /0x460 net/core/dst.c:124 rcu_do_batch kernel/rcu/tree.c:2569 [inline] rcu_core+0xafd/0x1830 kernel/rcu/tree. ---truncated--- **CVE ID: CVE-2024-44987**		
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following	https://git.kernel.org/stable/c/326a89321f9d5	O-LIN-LINU-190924/3434

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
			vulnerability has been resolved: net: ethernet: mtk_wed: fix use-after-free panic in mtk_wed_setup_tc_block_cb() When there are multiple ap interfaces on one band and with WED on, turning the interface down will cause a kernel panic on MT798X. Previously, cb_priv was freed in mtk_wed_setup_tc_block() without marking NULL,and mtk_wed_setup_tc_block_cb() didn't check the value, too. Assign NULL after free cb_priv in mtk_wed_setup_tc_block() and check NULL in mtk_wed_setup_tc_block_cb(). ----------	fe399fe6f9ff7c0fc766582a6a0, https://git.kernel.org/stable/c/b453a4bbda03aa8741279c360ac82d1c3ac33548, https://git.kernel.org/stable/c/db1b4bedb9b97c6d34b03d03815147c04fffe8b4	

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
			Unable to handle kernel paging request at virtual address 0072460bca32b4f5 Call trace: mtk_wed_setup_tc_block_cb+0x4/0x38 0xffffffc0794084bc tcf_block_playback_offloads+0x70/0x1e8 tcf_block_unbind+0x6c/0xc8 ... --------- **CVE ID: CVE-2024-44997**		
Out-of-bounds Write	11-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: s390/dasd: fix error recovery leading to data corruption on ESE devices Extent Space Efficient (ESE) or thin provisioned volumes need to be	https://git.kernel.org/stable/c/0a228896a1b3654cd461ff654f6a64e97a9c3246, https://git.kernel.org/stable/c/19f60a55b2fda49bc4f6134a5f6356ef62ee69d8, https://git.kernel.org/stable/c/5d4a304338daf83ace2887aaacafd66fe99ed5cc	O-LIN-LINU-190924/3435

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
			formatted on demand during usual IO processing. The dasd_ese_needs_format function checks for error codes that signal the non existence of a proper track format. The check for incorrect length is to imprecise since other error cases leading to transport of insufficient data also have this flag set. This might lead to data corruption in certain error cases for example during a storage server warmstart. Fix by removing the check for incorrect length and replacing by explicitly checking for invalid track format in transport mode.		

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
			Also remove the check for file protected since this is not a valid ESE handling case. **CVE ID: CVE-2024-45026**		
Use of Uninitialized Resource	04-Sep-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: validate vlan header Ensure there is sufficient room to access the protocol field of the VLAN header, validate it once before the flowtable lookup. ========== ========== ========== ======== BUG: KMSAN: uninit-value in nf_flow_offload_inet_hook+0x45a/0x5f0 net/netfilter/nf_flow_table_inet.c:32 nf_flow_offload_inet_hook+0x45a/0x5f0	https://git.kernel.org/stable/c/0279c35d242d037abeb73d60d06a6d1bb7f672d9, https://git.kernel.org/stable/c/043a18bb6cf16adaa2f8642acfde6e8956a9caaa, https://git.kernel.org/stable/c/6ea14ccb60c8ab829349979b22b58a941ec4a3ee	O-LIN-LINU-190924/3436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/netfilter/nf_flow_table_inet.c:32 nf_hook_entry_hookfn include/linux/netfilter.h:154 [inline] nf_hook_slow+0xf4/0x400 net/netfilter/core.c:626 nf_hook_ingress include/linux/netfilter_netdev.h:34 [inline] nf_ingress net/core/dev.c:5440 [inline] **CVE ID: CVE-2024-44983**		
Use of Uninitialized Resource	04-Sep-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: gtp: pull network headers in gtp_dev_xmit() syzbot/KMSAN reported use of uninit-value in get_dev_xmit() [1] We must make sure the IPv4 or Ipv6 header is pulled in skb->head	https://git.kernel.org/stable/c/137d565ab89ce3584503b443bc9e00d44f482593, https://git.kernel.org/stable/c/1f6b62392453d8f36685d19b761307a8c5617ac1, https://git.kernel.org/stable/c/34ba4f29f3d9eb52dee37512059efb2afd7e966f	O-LIN-LINU-190924/3437

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
			before accessing fields in them. Use pskb_inet_may_pull() to fix this issue. [1] BUG: KMSAN: uninit-value in ipv6_pdp_find drivers/net/gtp.c:220 [inline] BUG: KMSAN: uninit-value in gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] BUG: KMSAN: uninit-value in gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281 ipv6_pdp_find drivers/net/gtp.c:220 [inline] gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281 __netdev_start_xmit include/linux/netdevice.h:4913 [inline]		

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
			netdev_start_xmit include/linux/netdevice.h:4922 [inline] xmit_one net/core/dev.c:3580 [inline] dev_hard_start_xmit+0x247/0xa20 net/core/dev.c:3596 __dev_queue_xmit+0x358c/0x5610 net/core/dev.c:4423 dev_queue_xmit include/linux/netdevice.h:3105 [inline] packet_xmit+0x9c/0x6c0 net/packet/af_packet.c:276 packet_snd net/packet/af_packet.c:3145 [inline] packet_sendmsg+0x90e3/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+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
			x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hoo		

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
			k mm/slub.c:3994 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_node_noprof+0x6bf/0xb80 mm/slub.c:4080 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:583 __alloc_skb+0x363/0x7b0 net/core/skbuff.c:674 alloc_skb include/linux/skbuff.h:1320 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6526 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2815 packet_alloc_skb net/packet/af_packet.c:2994 [inline] packet_snd net/packet/af_packet.c:3088 [inline] packet_sendmsg+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
			x749c/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_		

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
			after_hwframe+0x77/0x7f CPU: 0 UID: 0 PID: 7115 Comm: syz.1.515 Not tainted 6.11.0-rc1-syzkaller-00043-g94ede2a3e913 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 **CVE ID: CVE-2024-44999**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bonding: fix xfrm real_dev null pointer dereference We shouldn't set real_dev to NULL because packets can be in transit and xfrm might call xdo_dev_offload_ok() in parallel. All callbacks assume real_dev is set.	https://git.kernel.org/stable/c/21816b696c172c19d53a30d45ee005cce246ed21, https://git.kernel.org/stable/c/2f72c6a66bcd7e0187ec085237fee5db27145294, https://git.kernel.org/stable/c/4582d4ff413a07d4ed8a4823c652dc5207760548	O-LIN-LINU-190924/3438

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
			Example trace: kernel: BUG: unable to handle page fault for address: 0000000000001030 kernel: bond0: (slave eni0np1): making interface the new active one kernel: #PF: supervisor write access in kernel mode kernel: #PF: error_code(0x0002) - not-present page kernel: PGD 0 P4D 0 kernel: Oops: 0002 [#1] PREEMPT SMP kernel: CPU: 4 PID: 2237 Comm: ping Not tainted 6.7.7+ #12 kernel: Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 kernel: RIP: 0010:nsim_ipsec_offload_ok+0xc/0x20 [netdevsim] kernel: bond0: (slave eni0np1):		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bond_ipsec_add_sa_all: failed to add SA kernel: Code: e0 0f 0b 48 83 7f 38 00 74 de 0f 0b 48 8b 47 08 48 8b 37 48 8b 78 40 e9 b2 e5 9a d7 66 90 0f 1f 44 00 00 48 8b 86 80 02 00 00 <83> 80 30 10 00 00 01 b8 01 00 00 00 c3 0f 1f 80 00 00 00 00 0f 1f kernel: bond0: (slave eni0np1): making interface the new active one kernel: RSP: 0018:ffffabde8155 3b98 EFLAGS: 00010246 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: kernel: RAX: 0000000000000000 RBX: ffff9eb404e74900 RCX: ffff9eb403d97c60 kernel: RDX: ffffffffc090de10 RSI: ffff9eb404e74900 RDI: ffff9eb3c5de9e00 kernel: RBP: ffff9eb3c0a42000 R08:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000010 R09: 0000000000000014 kernel: R10: 7974203030303030 R11: 3030303030303030 R12: 0000000000000000 kernel: R13: ffff9eb3c5de9e00 R14: ffffabde81553cc8 R15: ffff9eb404c53000 kernel: FS: 00007f2a77a3ad00(0000) GS:ffff9eb43bd00000(0000) knlGS:0000000000000000 kernel: CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 kernel: CR2: 0000000000001030 CR3: 00000001122ab000 CR4: 0000000000350ef0 kernel: bond0: (slave eni0np1): making interface the new active one kernel: Call Trace:		

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
			kernel: <TASK> kernel: ? __die+0x1f/0x60 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ? page_fault_oops+0x142/0x4c0 kernel: ? do_user_addr_fault+0x65/0x670 kernel: ? kvm_read_and_reset_apf_flags+0x3b/0x50 kernel: bond0: (slave eni0np1): making interface the new active one kernel: ? exc_page_fault+0x7b/0x180 kernel: ? asm_exc_page_fault+0x22/0x30 kernel: ? nsim_bpf_uninit+0x50/0x50 [netdevsim] kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ? nsim_ipsec_offload_ok+0xc/0x20 [netdevsim]		

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

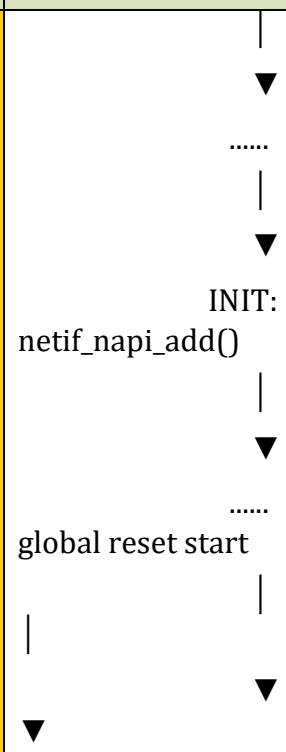
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel: bond0: (slave eni0np1): making interface the new active one kernel: bond_ipsec_offload_ok+0x7b/0x90 [bonding] kernel: xfrm_output+0x61/0x3b0 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ip_push_pending_frames+0x56/0x80 **CVE ID: CVE-2024-44989**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bonding: fix null pointer deref in bond_ipsec_offload_ok We must check if there is an active slave before dereferencing the pointer. **CVE ID: CVE-2024-44990**	https://git.kernel.org/stable/c/0707260a18312bbcd2a5668584e3692d0a29e3f6, https://git.kernel.org/stable/c/2f5bdd68c1ce64bda6bef4d361a3de23b04ccd59, https://git.kernel.org/stable/c/32a0173600c63aadaf2103bf02f074982e8602ab	O-LIN-LINU-190924/3439
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/195918217448	O-LIN-LINU-190924/3440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: net: hns3: fix a deadlock problem when config TC during resetting When config TC during the reset process, may cause a deadlock, the flow is as below: pf reset start ▼ ..... setup tc ▼ DOWN: napi_disable() napi_disable()(skip) ..... napi_enable() ▼ UINIT: netif_napi_del()	a6bb7f929d6a2ffffce9f1ece1cc, https://git.kernel.org/stable/c/67492d4d105c0a6321b00c393eec96b9a7a97a16, https://git.kernel.org/stable/c/6ae2b7d63cd056f363045eb65409143e16f23ae8	

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
			 In reset process, the driver will DOWN the port and then UINIT, in this case, the setup tc process will UP the port before UINIT, so cause the problem. Adds a DOWN process in UINIT to fix it.		

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
			CVE ID: CVE-2024-44995		
Uncontrolled Recursion	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: vsock: fix recursive ->recvmsg calls After a vsock socket has been added to a BPF sockmap, its prot->recvmsg has been replaced with vsock_bpf_recvmsg(). Thus the following recursiion could happen: vsock_bpf_recvmsg() -> __vsock_recvmsg() -> vsock_connectible_recvmsg() -> prot->recvmsg() -> vsock_bpf_recvmsg() again We need to fix it by calling the original ->recvmsg() without any BPF	https://git.kernel.org/stable/c/69139d2919dd4aa9a553c8245e7c63e82613e3fc, https://git.kernel.org/stable/c/921f1acf0c3cf6b1260ab57a8a6e8b3d5f3023d5, https://git.kernel.org/stable/c/b4ee8cf1acc5018ed1369150d7bb3e0d0f79e135	O-LIN-LINU-190924/3441

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
			sockmap logic in __vsock_recvmsg(). **CVE ID: CVE-2024-44996**		
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fs/netfs/fscache_cookie: add missing "n_accesses" check This fixes a NULL pointer dereference bug due to a data race which looks like this: BUG: kernel NULL pointer dereference, address: 0000000000000008 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] SMP PTI CPU: 33 PID: 16573 Comm: kworker/u97:799	https://git.kernel.org/stable/c/0a4d41fa14b2a0efd40e350cfe8ec6a4c998ac1d, https://git.kernel.org/stable/c/b8a50877f68efdcc0be3fcc5116e00c31b90e45b, https://git.kernel.org/stable/c/dfaa39b05a6cf34a16c525a2759ee6ab26b5fef6	O-LIN-LINU-190924/3442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Not tainted 6.8.7-cm4all1-hp+ #43 Hardware name: HP ProLiant DL380 Gen9/ProLiant DL380 Gen9, BIOS P89 10/17/2018 Workqueue: events_unbound netfs_rreq_write_to_cache_work RIP: 0010:cachefiles_prepare_write+0x30/0xa0 Code: 57 41 56 45 89 ce 41 55 49 89 cd 41 54 49 89 d4 55 53 48 89 fb 48 83 ec 08 48 8b 47 08 48 83 7f 10 00 48 89 34 24 48 8b 68 20 <48> 8b 45 08 4c 8b 38 74 45 49 8b 7f 50 e8 4e a9 b0 ff 48 8b 73 10 RSP: 0018:ffffb4e78113bde0 EFLAGS: 00010286 RAX: ffff976126be6d10 RBX: ffff97615cdb8438 RCX: 0000000000020000 RDX: ffff97605e6c4c68 RSI: ffff97605e6c4c60		

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
			RDI: ffff97615cdb8438 RBP: 0000000000000000 R08: 0000000000278333 R09: 0000000000000001 R10: ffff97605e6c4600 R11: 0000000000000001 R12: ffff97605e6c4c68 R13: 0000000000020000 R14: 0000000000000001 R15: ffff976064fe2c00 FS: 0000000000000000(0000) GS:ffff9776dfd40000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000008 CR3: 000000005942c002 CR4: 00000000001706f0 Call Trace: <TASK>		

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
			? __die+0x1f/0x70 ? page_fault_oops+0x15d/0x440 ? search_module_extables+0xe/0x40 ? fixup_exception+0x22/0x2f0 ? exc_page_fault+0x5f/0x100 ? asm_exc_page_fault+0x22/0x30 ? cachefiles_prepare_write+0x30/0xa0 netfs_rreq_write_to_cache_work+0x135/0x2e0 process_one_work+0x137/0x2c0 worker_thread+0x2e9/0x400 ? __pfx_worker_thread+0x10/0x10 kthread+0xcc/0x100 ? __pfx_kthread+0x10/0x10		

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
			ret_from_fork+0x30/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1b/0x30 </TASK> Modules linked in: CR2: 0000000000000008 ---[end trace 0000000000000000]--- This happened because fscache_cookie_state_machine() was slow and was still running while another process invoked fscache_unuse_cookie(); this led to a fscache_cookie_lru_do_one() call, setting the FSCACHE_COOKIE_DO_LRU_DISCARD flag, which was picked up by fscache_cookie_state_machine(), withdrawing the cookie via		

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

			cachefiles_withdraw_cookie(), clearing cookie->cache_priv.
			
			At the same time, yet another process invoked
			cachefiles_prepare_write(), which found a NULL pointer in this code
			line:
			
			struct cachefiles_object *object = cachefiles_cres_object(cres);
			
			The next line crashes, obviously:
			
			struct cachefiles_cache *cache = object->volume->cache;
			
			During cachefiles_prepare_write(), the "n_accesses" counter is
			non-zero (via fscache_begin_operation()). The cookie must not be
			withdrawn until it drops to zero.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The counter is checked by fscache_cookie_state_machine() before switching to FSCACHE_COOKIE_STATE_RELINQUISHING and FSCACHE_COOKIE_STATE_WITHDRAWING (in "case FSCACHE_COOKIE_STATE_FAILED"), but not for FSCACHE_COOKIE_STATE_LRU_DISCARDING ("case FSCACHE_COOKIE_STATE_ACTIVE"). This patch adds the missing check. With a non-zero access counter, the function returns and the next fscache_end_cookie_access() call will queue another fscache_cookie_state_machine() call to handle the still-pending FSCACHE_COOKIE_DO_LRU_DISCARD. **CVE ID: CVE-2024-45000**		

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
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: rtla/osnoise: Prevent NULL dereference in error handling If the "tool->data" allocation fails then there is no need to call osnoise_free_top() and, in fact, doing so will lead to a NULL dereference. **CVE ID: CVE-2024-45002**	https://git.kernel.org/stable/c/753f1745146e03abd17eec8eee95faffc96d743d, https://git.kernel.org/stable/c/90574d2a675947858b47008df8d07f75ea50d0d0, https://git.kernel.org/stable/c/abdb9ddaaab476e62805e36cce7b4ef8413ffd01	O-LIN-LINU-190924/3443
NULL Pointer Dereference	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: xhci: Fix Panther point NULL pointer deref at full-speed re-enumeration re-enumerating full-speed devices after a failed address device command can trigger a NULL pointer dereference.	https://git.kernel.org/stable/c/0f0654318e25b2c185e245ba4a591e42fabb5e59, https://git.kernel.org/stable/c/365ef7c4277fdd781a695c3553fa157d622d805d, https://git.kernel.org/stable/c/5ad898ae82412f8a689d59829804bff2999dd0ea	O-LIN-LINU-190924/3444

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
			Full-speed devices may need to reconfigure the endpoint 0 Max Packet Size value during enumeration. Usb core calls usb_ep0_reinit() in this case, which ends up calling xhci_configure_endpoint(). On Panther point xHC the xhci_configure_endpoint() function will additionally check and reserve bandwidth in software. Other hosts do this in hardware If xHC address device command fails then a new xhci_virt_device structure is allocated as part of re-enabling the slot, but the bandwidth table pointers are not set up properly here. This triggers the NULL pointer		

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
			dereference the next time usb_ep0_reinit() is called and xhci_configure_endpoint() tries to check and reserve bandwidth [46710.713538] usb 3-1: new full-speed USB device number 5 using xhci_hcd [46710.713699] usb 3-1: Device not responding to setup address. [46710.917684] usb 3-1: Device not responding to setup address. [46711.125536] usb 3-1: device not accepting address 5, error -71 [46711.125594] BUG: kernel NULL pointer dereference, address: 0000000000000008 [46711.125600] #PF: supervisor read access in kernel mode [46711.125603] #PF:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			error_code(0x0000) - not-present page [46711.125606] PGD 0 P4D 0 [46711.125610] Oops: Oops: 0000 [#1] PREEMPT SMP PTI [46711.125615] CPU: 1 PID: 25760 Comm: kworker/1:2 Not tainted 6.10.3_2 #1 [46711.125620] Hardware name: Gigabyte Technology Co., Ltd. [46711.125623] Workqueue: usb_hub_wq hub_event [usbcore] [46711.125668] RIP: 0010:xhci_reserve_bandwidth (drivers/usb/host/xhci.c Fix this by making sure bandwidth table pointers are set up correctly after a failed address device command, and additionally by avoiding checking for bandwidth in cases		

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
			like this where no actual endpoints are added or removed, i.e. only context for default control endpoint 0 is evaluated. **CVE ID: CVE-2024-45006**		
N/A	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: only decrement add_addr_accepted for MPJ req Adding the following warning ... WARN_ON_ONCE(msk->pm.add_addr_accepted == 0) ... before decrementing the add_addr_accepted counter helped to find a bug when running the "remove single subflow" subtest from the	https://git.kernel.org/stable/c/1c1f721375989579e46741f59523e39ec9b2a9bd, https://git.kernel.org/stable/c/2060f1efab370b496c4903b840844ecaff324c3c, https://git.kernel.org/stable/c/35b31f5549ede4070566b949781e83495906b43d	O-LIN-LINU-190924/3445

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
			mptcp_join.sh selftest. Removing a 'subflow' endpoint will first trigger a RM_ADDR, then the subflow closure. Before this patch, and upon the reception of the RM_ADDR, the other peer will then try to decrement this add_addr_accepted. That's not correct because the attached subflows have not been created upon the reception of an ADD_ADDR. A way to solve that is to decrement the counter only if the attached subflow was an MP_JOIN to a remote id that was not 0, and initiated by the host receiving the RM_ADDR. **CVE ID: CVE-2024-45009**		
N/A	11-Sep-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/322ea3778965	O-LIN-LINU-190924/3446

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
			vulnerability has been resolved: mptcp: pm: only mark 'subflow' endp as available Adding the following warning ... WARN_ON_ONCE(msk->pm.local_addr_used == 0) ... before decrementing the local_addr_used counter helped to find a bug when running the "remove single address" subtest from the mptcp_join.sh selftests. Removing a 'signal' endpoint will trigger the removal of all subflows linked to this endpoint via mptcp_pm_nl_rm_addr_or_subflow() with	da72862cca2a0c50253aacf65fe6, https://git.kernel.org/stable/c/43cf912b0b0fc7b4fd12cbc735d1f5afb8e1322d, https://git.kernel.org/stable/c/7fdc870d08960961408a44c569f20f50940e7d4f	

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
			rm_type == MPTCP_MIB_RMSUBFLOW. This will decrement the local_addr_used counter, which is wrong in this case because this counter is linked to 'subflow' endpoints, and here it is a 'signal' endpoint that is being removed. Now, the counter is decremented, only if the ID is being used outside of mptcp_pm_nl_rm_addr_or_subflow(), only for 'subflow' endpoints, and if the ID is not 0 -- local_addr_used is not taking into account these ones. This marking of the ID as being available, and the decrement is done no matter if a subflow using this ID is currently available, because the subflow could have been closed before.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45010		
N/A	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: char: xillybus: Check USB endpoints when probing device Ensure, as the driver probes the device, that all endpoints that the driver may attempt to access exist and are of the correct type. All XillyUSB devices must have a Bulk IN and Bulk OUT endpoint at address 1. This is verified in xillyusb_setup_base_eps(). On top of that, a XillyUSB device may have additional Bulk OUT endpoints. The information about these endpoints' addresses is deduced	https://git.kernel.org/stable/c/1371d32b95972d39c1e6e4bae8b6d0df1b573731, https://git.kernel.org/stable/c/2374bf7558de915edc6ec8cb10ec3291dfab9594, https://git.kernel.org/stable/c/25ee8b2908200fc862c0434e5ad483817d50ceda	O-LIN-LINU-190924/3447

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
			from a data structure (the IDT) that the driver fetches from the device while probing it. These endpoints are checked in setup_channels(). A XillyUSB device never has more than one IN endpoint, as all data towards the host is multiplexed in this single Bulk IN endpoint. This is why setup_channels() only checks OUT endpoints. **CVE ID: CVE-2024-45011**		
Allocation of Resources Without Limits or Throttling	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nouveau/firmware: use dma non-coherent allocator Currently, enabling SG_DEBUG in the kernel will cause nouveau to hit a BUG() on startup, when the iommu is enabled:	https://git.kernel.org/stable/c/57ca481fca97ca4553e8c85d6a94baf4cb40c40e, https://git.kernel.org/stable/c/9b340aeb26d50e9a9ec99599e2a39b035fac978e, https://git.kernel.org/stable/c/cc29c5546c6a373648363ac49781f1d74b530707	O-LIN-LINU-190924/3448

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
			kernel BUG at include/linux/scatterlist.h:187! invalid opcode: 0000 [#1] PREEMPT SMP NOPTI CPU: 7 PID: 930 Comm: (udev-worker) Not tainted 6.9.0-rc3Lyude-Test+ #30 Hardware name: MSI MS-7A39/A320M GAMING PRO (MS-7A39), BIOS 1.I0 01/22/2019 RIP: 0010:sg_init_one+0x85/0xa0 Code: 69 88 32 01 83 e1 03 f6 c3 03 75 20 a8 01 75 1e 48 09 cb 41 89 54 24 08 49 89 1c 24 41 89 6c 24 0c 5b 5d 41 5c e9 7b b9 88 00 <0f> 0b 0f 0b 0f 0b 48 8b 05 5e 46 9a 01 eb b2 66 66 2e 0f 1f 84 00 RSP: 0018:ffffa776017bf6a0 EFLAGS: 00010246 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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffffa77600d87000 RCX: 000000000000002b RDX: 0000000000000001 RSI: 0000000000000000 RDI: ffffa77680d87000 RBP: 000000000000e000 R08: 0000000000000000 R09: 0000000000000000 R10: ffff98f4c46aa508 R11: 0000000000000000 R12: ffff98f4c46aa508 R13: ffff98f4c46aa008 R14: ffffa77600d4a000 R15: ffffa77600d4a018 FS: 00007feeb5aae980(0000) GS:ffff98f5c4dc0000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f22cb9a452		

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 CR3: 00000001043ba000 CR4: 00000000003506f0 Call Trace: <TASK> ? die+0x36/0x90 ? do_trap+0xdd/0x100 ? sg_init_one+0x85/0xa0 ? do_error_trap+0x65/0x80 ? sg_init_one+0x85/0xa0 ? exc_invalid_op+0x50/0x70 ? sg_init_one+0x85/0xa0 ? asm_exc_invalid_op+0x1a/0x20 ? sg_init_one+0x85/0xa0 nvkm_firmware_ctor+0x14a/0x250 [nouveau] nvkm_falcon_fw_ct		

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
			or+0x42/0x70 [nouveau] ga102_gsp_booter_ctor+0xb4/0x1a0 [nouveau] r535_gsp_oneinit+0xb3/0x15f0 [nouveau] ? srso_return_thunk+0x5/0x5f ? srso_return_thunk+0x5/0x5f ? nvkm_udevice_new+0x95/0x140 [nouveau] ? srso_return_thunk+0x5/0x5f ? srso_return_thunk+0x5/0x5f ? ktime_get+0x47/0xb0 Fix this by using the non-coherent allocator instead, I think there might be a better answer to this, but it involve ripping up some of APIs using sg lists.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45012		
Use After Free	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nvme: move stopping keep-alive into nvme_uninit_ctrl() Commit 4733b65d82bd ("nvme: start keep-alive after admin queue setup") moves starting keep-alive from nvme_start_ctrl() into nvme_init_ctrl_finish(), but don't move stopping keep-alive into nvme_uninit_ctrl(), so keep-alive work can be started and keep pending after failing to start controller, finally use-after-free is triggered if nvme host driver is unloaded. This patch fixes kernel panic when running nvme/004	https://git.kernel.org/stable/c/4101af98ab573554c4225e328d506fec2a74bc54, https://git.kernel.org/stable/c/a54a93d0e3599b05856971734e15418ac551a14c	O-LIN-LINU-190924/3449

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
			in case that connection failure is triggered, by moving stopping keep-alive into nvme_uninit_ctrl(). This way is reasonable because keep-alive is now started in nvme_init_ctrl_finish(). **CVE ID: CVE-2024-45013**		
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/msm/dpu: move dpu_encoder's connector assignment to atomic_enable() For cases where the crtc's connectors_changed was set without enable/active getting toggled , there is an atomic_enable() call followed by an atomic_disable() but without an atomic_mode_set().	https://git.kernel.org/stable/c/3bacf814b6a61cc683c68465f175ebd938f09c52, https://git.kernel.org/stable/c/3fb61718bcbe309279205d1cc275a6435611dc77, https://git.kernel.org/stable/c/aedf02e46eb549dac8db4821a6b9f0c6bf6e3990	O-LIN-LINU-190924/3450

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
			This results in a NULL ptr access for the dpu_encoder_get_drm_fmt() call in the atomic_enable() as the dpu_encoder's connector was cleared in the atomic_disable() but not re-assigned as there was no atomic_mode_set() call. Fix the NULL ptr access by moving the assignment for atomic_enable() and also use drm_atomic_get_new_connector_for_encoder() to get the connector from the atomic_state. Patchwork: https://patchwork.freedesktop.org/patch/606729/ **CVE ID: CVE-2024-45015**		
Use After Free	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/0486d31dd8198e22b63a4730244b38fffce6d4	O-LIN-LINU-190924/3451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			netem: fix return value if duplicate enqueue fails There is a bug in netem_enqueue() introduced by commit 5845f706388a ("net: netem: fix skb length BUG_ON in __skb_to_sgvec") that can lead to a use-after-free. This commit made netem_enqueue() always return NET_XMIT_SUCCESS when a packet is duplicated, which can cause the parent qdisc's q.qlen to be mistakenly incremented. When this happens qlen_notify() may be skipped on the parent during destruction, leaving a dangling pointer for some classful qdiscs like DRR. There are two ways for the bug happen:	69, https://git.kernel.org/stable/c/52d99a69f3d556c6426048c9d481b912205919d8, https://git.kernel.org/stable/c/577d6c0619467fe90f7e8e57e45cb5bd9d936014	

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
			- If the duplicated packet is dropped by rootq->enqueue() and then the original packet is also dropped. - If rootq->enqueue() sends the duplicated packet to a different qdisc and the original packet is dropped. In both cases NET_XMIT_SUCCESS is returned even though no packets are enqueued at the netem qdisc. The fix is to defer the enqueue of the duplicate packet until after the original packet has been guaranteed to return NET_XMIT_SUCCESS. **CVE ID: CVE-2024-45016**		
N/A	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/2ae52a65a850ded75a94e8d7ec1e09737f4c650	O-LIN-LINU-190924/3452

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
			net/mlx5: Fix IPsec RoCE MPV trace call Prevent the call trace below from happening, by not allowing IPsec creation over a slave, if master device doesn't support IPsec. WARNING: CPU: 44 PID: 16136 at kernel/locking/rwsem.c:240 down_read+0x75/0x94 Modules linked in: esp4_offload esp4 act_mirred act_vlan cls_flower sch_ingress mlx5_vdpa vringh vhost_iotlb vdpa mst_pciconf(OE) nfsv3 nfs_acl nfs lockd grace fscache netfs xt_CHECKSUM xt_MASQUERADE xt_conntrack ipt_REJECT nf_reject_ipv4 nft_compat nft_counter nft_chain_nat nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4	9, https://git.kernel.org/stable/c/607e1df7bd47fe91cab85a97f57870a26d066137	

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
			rfkill cuse fuse rpcrdma sunrpc rdma_ucm ib_srpt ib_isert iscsi_target_mod target_core_mod ib_umad ib_iser libiscsi scsi_transport_iscsi rdma_cm ib_ipoib iw_cm ib_cm ipmi_ssif intel_rapl_msr intel_rapl_common amd64_edac edac_mce_amd kvm_amd kvm irqbypass crct10dif_pclmul crc32_pclmul mlx5_ib ghash_clmulni_intel sha1_ssse3 dell_smbios ib_uverbs aesni_intel crypto_simd dcdbas wmi_bmof dell_wmi_descriptor cryptd pcspkr ib_core acpi_ipmi sp5100_tco ccp i2c_piix4 ipmi_si ptdma k10temp ipmi_devintf ipmi_msghandler acpi_power_meter acpi_cpufreq ext4 mbcache jbd2 sd_mod t10_pi sg mgag200 drm_kms_helper syscopyarea sysfillrect		

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
			mlx5_core sysimgblt fb_sys_fops cec ahci libahci mlxfw drm pci_hyperv_intf libata tg3 sha256_ssse3 tls megaraid_sas i2c_algo_bit psample wmi dm_mirror dm_region_hash dm_log dm_mod [last unloaded: mst_pci] CPU: 44 PID: 16136 Comm: kworker/44:3 Kdump: loaded Tainted: GOE 5.15.0-20240509.el8uek.uek7_u3_update_v6.6_ipsec_bf.x86_64 #2 Hardware name: Dell Inc. PowerEdge R7525/074H08, BIOS 2.0.3 01/15/2021 Workqueue: events xfrm_state_gc_task RIP: 0010:down_read+0x75/0x94 Code: 00 48 8b 45 08 65 48 8b 14 25 80 fc 01 00 83 e0 02 48 09 d0 48 83 c8 01 48 89 45 08 5d		

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
			31 c0 89 c2 89 c6 89 c7 e9 cb 88 3b 00 <0f> 0b 48 8b 45 08 a8 01 74 b2 a8 02 75 ae 48 89 c2 48 83 ca 02 f0 RSP: 0018:ffffb26387773da8 EFLAGS: 00010282 RAX: 0000000000000000 RBX: ffffa08b658af900 RCX: 0000000000000001 RDX: 0000000000000000 RSI: ff886bc5e1366f2f RDI: 0000000000000000 RBP: ffffa08b658af940 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffffa0a9bfb31540 R13: ffffa0a9bfb37900 R14: 0000000000000000		

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 R15: ffffa0a9bfb37905 FS: 0000000000000000(0000) GS:ffffa0a9bfb00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000055a45ed814e8 CR3: 000000109038a000 CR4: 0000000000350ee0 Call Trace: <TASK> ? show_trace_log_lvl+0x1d6/0x2f9 ? show_trace_log_lvl+0x1d6/0x2f9 ? mlx5_devcom_for_each_peer_begin+0x29/0x60 [mlx5_core] ? down_read+0x75/0x94 ? __warn+0x80/0x113		

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
			? down_read+0x75/0x94 ? report_bug+0xa4/0x11d ? handle_bug+0x35/0x8b ? exc_invalid_op+0x14/0x75 ? asm_exc_invalid_op+0x16/0x1b ? down_read+0x75/0x94 ? down_read+0xe/0x94 mlx5_devcom_for_each_peer_begin+0x29/0x60 [mlx5_core] mlx5_ipsec_fs_roce_tx_destroy+0xb1/0x130 [mlx5_core] tx_destroy+0x1b/0xc0 [mlx5_core] tx_ft_put+0x53/0xc0 [mlx5_core] mlx5e_xfrm_free_state+0x45/0x90 [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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__xfrm_state_destroy+0x10f/0x1a2 xfrm_state_gc_task+0x81/0xa9 process_one_work+0x1f1/0x3c6 worker_thread+0x53/0x3e4 ? process_one_work.cold+0x46/0x3c kthread+0x127/0x144 ? set_kthread_struct+0x60/0x52 ret_from_fork+0x22/0x2d </TASK> ---[end trace 5ef7896144d398e1]--- **CVE ID: CVE-2024-45017**		
Improper Initialization	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: initialise extack before use	https://git.kernel.org/stable/c/119be227bc04f5035efa64cb823b8a5ca5e2d1c1, https://git.kernel.org/stable/c/356beb911b63a8cff34cb57f75	O-LIN-LINU-190924/3453

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
			Fix missing initialisation of extack in flow offload. **CVE ID: CVE-2024-45018**	5c2a2d2ee9dec7, https://git.kernel.org/stable/c/7eafeec6be68ebd6140a830ce9ae68ad5b67ec78	
Improper Locking	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Take state lock during tx timeout reporter mlx5e_safe_reopen_channels() requires the state lock taken. The referenced changed in the Fixes tag removed the lock to fix another issue. This patch adds it back but at a later point (when calling mlx5e_safe_reopen_channels()) to avoid the deadlock referenced in the Fixes tag. **CVE ID: CVE-2024-45019**	https://git.kernel.org/stable/c/03d3734bd692affe4d0e9c9d638f491aaf37411b, https://git.kernel.org/stable/c/8e57e66ecbdd2fddc9fbf3e984b1c523b70e9809, https://git.kernel.org/stable/c/b3b9a87adee97854bcd71057901d46943076267e	O-LIN-LINU-190924/3454
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/6e3987ac310c74bb4dd6a2fa8e46702fe505fb2	O-LIN-LINU-190924/3455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bpf: Fix a kernel verifier crash in stacksafe() Daniel Hodges reported a kernel verifier crash when playing with sched-ext. Further investigation shows that the crash is due to invalid memory access in stacksafe(). More specifically, it is the following code: if (exact != NOT_EXACT && old->stack[spi].slot_type[i % BPF_REG_SIZE] != cur->stack[spi].slot_type[i % BPF_REG_SIZE]) return false; The 'i' iterates old->allocated_stack. If cur->allocated_stack < old->allocated_stack the out-of-bound access will happen.	b, https://git.kernel.org/stable/c/7cad3174cc79519bf5f6c4441780264416822c08, https://git.kernel.org/stable/c/bed2eb964c70b780fb55925892a74f26cb590b25	

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
			To fix the issue add 'i >= cur->allocated_stack' check such that if the condition is true, stacksafe() should fail. Otherwise, cur->stack[spi].slot_type[i % BPF_REG_SIZE] memory access is legal. **CVE ID: CVE-2024-45020**		
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: memcg_write_event_control(): fix a user-triggerable oops we are *not* guaranteed that anything past the terminating NUL is mapped (let alone initialized with anything sane). **CVE ID: CVE-2024-45021**	https://git.kernel.org/stable/c/046667c4d3196938e992fba0dfcde570aa85cd0e, https://git.kernel.org/stable/c/0fbe2a72e853a1052abe9bc2b7df8ddb102da227, https://git.kernel.org/stable/c/1b37ec85ad95b612307627758c6018cd9d92cca8	O-LIN-LINU-190924/3456
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/61ebe5a747da6	O-LIN-LINU-190924/3457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: mm/vmalloc: fix page mapping if vm_area_alloc_pages() with high order fallback to order 0 The __vmap_pages_range_noflush() assumes its argument pages** contains pages with the same page shift. However, since commit e9c3cda4d86e ("mm, vmalloc: fix high order __GFP_NOFAIL allocations"), if gfp_flags includes __GFP_NOFAIL with high order in vm_area_alloc_pages() and page allocation failed for high order, the pages** may contain two different page shifts (high order and order-0). This could lead __vmap_pages_range_noflush() to	49057c37be1c37eb934b4af79ca, https://git.kernel.org/stable/c/c91618816f4d21fc574d7577a37722adcd4075b2, https://git.kernel.org/stable/c/de7bad86345c43cd040ed43e20d9fad78a3ee59f	

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
			perform incorrect mappings, potentially resulting in memory corruption. Users might encounter this as follows (vmap_allow_huge = true, 2M is for PMD_SIZE): kvmalloc(2M, __GFP_NOFAIL|GFP_X) __vmalloc_node_range_noprof(vm_flags=VM_ALLOW_HUGE_VMAP) vm_area_alloc_pages(order=9) ---> order-9 allocation failed and fallback to order-0 vmap_pages_range() vmap_pages_range_noflush() __vmap_pages_range_noflush(page_shift = 21) ----> wrong mapping happens		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			We can remove the fallback code because if a high-order allocation fails, __vmalloc_node_range_noprof() will retry with order-0. Therefore, it is unnecessary to fallback to order-0 here. Therefore, fix this by removing the fallback code. **CVE ID: CVE-2024-45022**		
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fix bitmap corruption on close_range() with CLOSE_RANGE_UNSHARE copy_fd_bitmaps(new, old, count) is expected to copy the first count/BITS_PER_LONG bits from old->full_fds_bits[] and fill the rest with zeroes. What it does is copying enough words	https://git.kernel.org/stable/c/5053581fe5dfb09b58c65dd8462bf5dea71f41ff, https://git.kernel.org/stable/c/8cad3b2b3ab81ca55f37405ffd1315bcc2948058, https://git.kernel.org/stable/c/9a2fa1472083580b6c66bdaf291f591e1170123a	O-LIN-LINU-190924/3458

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
			(BITS_TO_LONGS(count/BITS_PER_LONG)), then memsets the rest. That works fine, *if* all bits past the cutoff point are clear. Otherwise we are risking garbage from the last word we'd copied. For most of the callers that is true - expand_fdtable() has count equal to old->max_fds, so there's no open descriptors past count, let alone fully occupied words in ->open_fds[], which is what bits in ->full_fds_bits[] correspond to. The other caller (dup_fd()) passes sane_fdtable_size(old_fdt, max_fds), which is the smallest multiple of BITS_PER_LONG that covers all opened descriptors below max_fds. In		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the common case (copying on fork()) max_fds is ~0U, so all opened descriptors will be below it and we are fine, by the same reasons why the call in expand_fdtable() is safe. Unfortunately, there is a case where max_fds is less than that and where we might, indeed, end up with junk in ->full_fds_bits[] - close_range(from, to, CLOSE_RANGE_UNSHARE) with * descriptor table being currently shared * 'to' being above the current capacity of descriptor table * 'from' being just under some chunk of opened descriptors. In that case we end up with observably		

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
			wrong behaviour - e.g. spawn a child with CLONE_FILES, get all descriptors in range 0..127 open, then close_range(64, ~0U, CLOSE_RANGE_UNSHARE) and watch dup(0) ending up with descriptor #128, despite #64 being observably not open. The minimally invasive fix would be to deal with that in dup_fd(). If this proves to add measurable overhead, we can go that way, but let's try to fix copy_fd_bitmaps() first. * new helper: bitmap_copy_and_expand(to, from, bits_to_copy, size). * make copy_fd_bitmaps() take the bitmap size in words, rather than bits; it's 'count' argument is always		

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
			a multiple of BITS_PER_LONG, so we are not losing any information, and that way we can use the same helper for all three bitmaps - compiler will see that count is a multiple of BITS_PER_LONG for the large ones, so it'll generate plain memcpy()+memset(). Reproducer added to tools/testing/selftests/core/close_range_test.c **CVE ID: CVE-2024-45025**		
Improper Initialization	02-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fuse: Initialize beyond-EOF page contents before setting uptodate fuse_notify_store(), unlike fuse_do_readpage(), does not enable page	https://git.kernel.org/stable/c/18a067240817bee8a9360539af5d79a4bf5398a5, https://git.kernel.org/stable/c/33168db352c7b56ae18aa55c2cae1a1c5905d30e, https://git.kernel.org/stable/c/3c0da3d163eb3	O-LIN-LINU-190924/3459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			zeroing (because it can be used to change partial page contents). So fuse_notify_store() must be more careful to fully initialize page contents (including parts of the page that are beyond end-of-file) before marking the page uptodate. The current code can leave beyond-EOF page contents uninitialized, which makes these uninitialized page contents visible to userspace via mmap(). This is an information leak, but only affects systems which do not enable init-on-alloc (via CONFIG_INIT_ON_ALLOC_DEFAULT_ON=y or the corresponding kernel command line parameter).	2f1f91891efaade027fa9b245b9	

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
			CVE ID: CVE-2024-44947		
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mmc: mmc_test: Fix NULL dereference on allocation failure If the "test->highmem = alloc_pages()" allocation fails then calling __free_pages(test->highmem) will result in a NULL dereference. Also change the error code to -ENOMEM instead of returning success. **CVE ID: CVE-2024-45028**	https://git.kernel.org/stable/c/2b507b03991f44dfb202fc2a82c9874d1b1f0c06, https://git.kernel.org/stable/c/3b4e76ceae5b5a46c968bd952f551ce173809f63, https://git.kernel.org/stable/c/9b9ba386d7bfdbc38445932c90fa9444c0524bea	O-LIN-LINU-190924/3460
Improper Locking	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: i2c: tegra: Do not mark ACPI devices as irq safe On ACPI machines, the tegra i2c	https://git.kernel.org/stable/c/14d069d92951a3e150c0a81f2ca3b93e54da913b, https://git.kernel.org/stable/c/2853e1376d8161b04c9ff18ba82b43f08a049905, https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module encounters an issue due to a mutex being called inside a spinlock. This leads to the following bug: BUG: sleeping function called from invalid context at kernel/locking/mutex.c:585 ... Call trace: __might_sleep __mutex_lock_common mutex_lock_nested acpi_subsys_runtime_resume rpm_resume tegra_i2c_xfer The problem arises because during __pm_runtime_resume(), the spinlock &dev->power.lock is acquired before rpm_resume() is called. Later, rpm_resume() invokes acpi_subsys_runtim	6861faf4232e4b78878f2de1ed3ee324ddae2287	

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
			e_resume(), which relies on mutexes, triggering the error. To address this issue, devices on ACPI are now marked as not IRQ-safe, considering the dependency of acpi_subsys_runtime_resume() on mutexes. **CVE ID: CVE-2024-45029**		
Out-of-bounds Write	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: igb: cope with large MAX_SKB_FRAGS Sabrina reports that the igb driver does not cope well with large MAX_SKB_FRAG values: setting MAX_SKB_FRAG to 45 causes payload corruption on TX. An easy reproducer is to run ssh to connect to the machine. With	https://git.kernel.org/stable/c/8aba27c4a5020abdf60149239198297f88338a8d, https://git.kernel.org/stable/c/8ea80ff5d8298356d28077bc30913ed37df65109, https://git.kernel.org/stable/c/b52bd8bcb9e8ff250c79b44f9af8b15cae8911ab	O-LIN-LINU-190924/3462

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
			MAX_SKB_FRAGS=17 it works, with MAX_SKB_FRAGS=45 it fails. This has been reported originally in https://bugzilla.redhat.com/show_bug.cgi?id=2265320 The root cause of the issue is that the driver does not take into account properly the (possibly large) shared info size when selecting the ring layout, and will try to fit two packets inside the same 4K page even when the 1st fraglist will trump over the 2nd head. Address the issue by checking if 2K buffers are insufficient. **CVE ID: CVE-2024-45030**		
NULL Pointer Dereference	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: cfg80211: Handle	https://git.kernel.org/stable/c/1f566eb912d192c83475a919331aea59619e1197, https://git.kern	O-LIN-LINU-190924/3463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSID based pmksa deletion wpa_supplicant 2.11 sends since 1efdba5fdc2c ("Handle PMKSA flush in the driver for SAE/OWE offload cases") SSID based PMKSA del commands. brcmfmac is not prepared and tries to dereference the NULL bssid and pmkid pointers in cfg80211_pmksa. PMKID_V3 operations support SSID based updates so copy the SSID. **CVE ID: CVE-2024-46672**	el.org/stable/c/2ad4e1ada8eebafa2d75a4b75eeeca882de6ada1, https://git.kernel.org/stable/c/4291f94f8c6b01505132c22ee27b59ed27c3584f	
Affected Version(s): From (including) 6.7 Up to (excluding) 6.10.8					
Double Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: scsi: aacraid: Fix double-free on probe failure aac_probe_one() calls hardware-specific init	https://git.kernel.org/stable/c/4b540ec7c0045c2d01c4e479f34bbc8f147afa4c, https://git.kernel.org/stable/c/564e1986b00c5f05d75342f8407f75f0a17b94df, https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functions through the aac_driver_ident::init pointer, all of which eventually call down to aac_init_adapter(). If aac_init_adapter() fails after allocating memory for aac_dev::queues, it frees the memory but does not clear that member. After the hardware-specific init function returns an error, aac_probe_one() goes down an error path that frees the memory pointed to by aac_dev::queues, resulting.in a double-free. **CVE ID: CVE-2024-46673**	60962c3d8e18e5d8dfa16df788974dd7f35bd87a	
Use After Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: dwc3: st: fix probed platform device ref count on probe error path	https://git.kernel.org/stable/c/060f41243ad7f6f5249fa7290dda0c01f723d12d, https://git.kernel.org/stable/c/1de989668708ce5875efc9d66	O-LIN-LINU-190924/3465

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 probe function never performs any paltform device allocation, thus error path "undo_platform_dev_alloc" is entirely bogus. It drops the reference count from the platform device being probed. If error path is triggered, this will lead to unbalanced device reference counts and premature release of device resources, thus possible use-after-free when releasing remaining devm-managed resources. **CVE ID: CVE-2024-46674**	9d227212aeb9a90, https://git.kernel.org/stable/c/4c6735299540f3c82a5033d35be76a5c42e0fb18	
Double Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix a use-after-free when hitting errors inside btrfs_submit_chunk()	https://git.kernel.org/stable/c/10d9d8c3512f16cad47b2ff81ec6fc4b27d8ee10, https://git.kernel.org/stable/c/4a3b9e1a8e6cd1a8d427a905e159de58d38941cc, https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3466

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
			[BUG] There is an internal report that KASAN is reporting use-after-free, with the following backtrace: BUG: KASAN: slab-use-after-free in btrfs_check_read_bio+0xa68/0xb70 [btrfs] Read of size 4 at addr ffff8881117cec28 by task kworker/u16:2/45 CPU: 1 UID: 0 PID: 45 Comm: kworker/u16:2 Not tainted 6.11.0-rc2-next-20240805-default+ #76 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.2-3-gd478f380-rebuilt.opensuse.org 04/01/2014 Workqueue: btrfs-endio btrfs_end_bio_work [btrfs] Call Trace: dump_stack_lvl+0x61/0x80	51722b99f41f5e722ffa10b8f61e802a0e70b331	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			print_address_description.constprop.0+0x5e/0x2f0 print_report+0x118/0x216 kasan_report+0x11d/0x1f0 btrfs_check_read_bio+0xa68/0xb70 [btrfs] process_one_work+0xce0/0x12a0 worker_thread+0x717/0x1250 kthread+0x2e3/0x3c0 ret_from_fork+0x2d/0x70 ret_from_fork_asm+0x11/0x20 Allocated by task 20917: kasan_save_stack+0x37/0x60 kasan_save_track+0x10/0x30		

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
			__kasan_slab_alloc+0x7d/0x80 kmem_cache_alloc_noprof+0x16e/0x3e0 mempool_alloc_noprof+0x12e/0x310 bio_alloc_bioset+0x3f0/0x7a0 btrfs_bio_alloc+0x2e/0x50 [btrfs] submit_extent_page+0x4d1/0xdb0 [btrfs] btrfs_do_readpage+0x8b4/0x12a0 [btrfs] btrfs_readahead+0x29a/0x430 [btrfs] read_pages+0x1a7/0xc60 page_cache_ra_unbounded+0x2ad/0x560 filemap_get_pages+0x629/0xa20 filemap_read+0x335/0xbf0		

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
			vfs_read+0x790/0xcb0 ksys_read+0xfd/0x1d0 do_syscall_64+0x6d/0x140 entry_SYSCALL_64_after_hwframe+0x4b/0x53 Freed by task 20917: kasan_save_stack+0x37/0x60 kasan_save_track+0x10/0x30 kasan_save_free_info+0x37/0x50 __kasan_slab_free+0x4b/0x60 kmem_cache_free+0x214/0x5d0 bio_free+0xed/0x180 end_bbio_data_read+0x1cc/0x580 [btrfs] btrfs_submit_chunk		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			+0x98d/0x1880 [btrfs] btrfs_submit_bio+0x33/0x70 [btrfs] submit_one_bio+0xd4/0x130 [btrfs] submit_extent_page+0x3ea/0xdb0 [btrfs] btrfs_do_readpage+0x8b4/0x12a0 [btrfs] btrfs_readahead+0x29a/0x430 [btrfs] read_pages+0x1a7/0xc60 page_cache_ra_unbounded+0x2ad/0x560 filemap_get_pages+0x629/0xa20 filemap_read+0x335/0xbf0 vfs_read+0x790/0xcb0 ksys_read+0xfd/0x1d0		

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
			do_syscall_64+0x6d/0x140 entry_SYSCALL_64_after_hwframe+0x4b/0x53 [CAUSE] Although I cannot reproduce the error, the report itself is good enough to pin down the cause. The call trace is the regular endio workqueue context, but the free-by-task trace is showing that during btrfs_submit_chunk() we already hit a critical error, and is calling btrfs_bio_end_io() to error out. And the original endio function called bio_put() to free the whole bio. This means a double freeing thus		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing use-after-free, e.g.: 1. Enter btrfs_submit_bio() with a read bio The read bio length is 128K, crossing two 64K stripes. 2. The first run of btrfs_submit_chunk () 2.1 Call btrfs_map_block(), which returns 64K 2.2 Call btrfs_split_bio() Now there are two bios, one referring to the first 64K, the other referring to the second 64K. 2.3 The first half is submitted. 3. The second run of btrfs_submit_chunk () 3.1 Call btrfs_map_block(), which by somehow failed		

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
			Now we call btrfs_bio_end_io() to handle the error 3.2 btrfs_bio_end_io() calls the original endio function Which is end_bbio_data_read(), and it calls bio_put() for the original bio. Now the original bio is freed. 4. The submitted first 64K bio finished Now we call into btrfs_check_read_bio() and tries to advance the bio iter. But since the original bio (thus its iter) is already freed, we trigger the above use-after free. And even if the memory is not poisoned/corrupted, we will later call the original endio function, causing a double freeing.		

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
			[FIX] Instead of calling btrfs_bio_end_io(), call btrfs_orig_bbio_end_io(), which has the extra check on split bios and do the pr ---truncated--- **CVE ID: CVE-2024-46687**		
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: gtp: fix a potential NULL pointer dereference When sockfd_lookup() fails, gtp_encap_enable_socket() returns a NULL pointer, but its callers only check for error pointers thus miss the NULL pointer case. Fix it by returning an error pointer with the error code carried from sockfd_lookup().	https://git.kernel.org/stable/c/28c67f0f84f889fe9f4cbda8354132b20dc9212d, https://git.kernel.org/stable/c/4643b91691e969b1b9ad54bf552d7a990cfa3b87, https://git.kernel.org/stable/c/612edd35f2a3910ab1f61c1f2338889d4ba99fa2	O-LIN-LINU-190924/3467

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
			(I found this bug during code inspection.) **CVE ID: CVE-2024-46677**		
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: pinctrl: single: fix potential NULL dereference in pcs_get_function() pinmux_generic_get_function() can return NULL and the pointer 'function' was dereferenced without checking against NULL. Add checking of pointer 'function' in pcs_get_function(). Found by code review. **CVE ID: CVE-2024-46685**	https://git.kernel.org/stable/c/0a2bab5ed161318f57134716accba0a30f3af191, https://git.kernel.org/stable/c/1c38a62f15e595346a1106025722869e87ffe044, https://git.kernel.org/stable/c/292151af6add3e5ab11b2e9916cffa5f52859a1f	O-LIN-LINU-190924/3468
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: smb/client: avoid dereferencing	https://git.kernel.org/stable/c/6df57c63c200cd05e085c3b695128260e21959b7, https://git.kernel.org/stable/c/	O-LIN-LINU-190924/3469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rdata=NULL in smb2_new_read_req() This happens when called from SMB2_read() while using rdma and reaching the rdma_readwrite_threshold. **CVE ID: CVE-2024-46686**	a01859dd6aebf826576513850a3b05992809e9d2, https://git.kernel.org/stable/c/b902fb78ab21299e4dd1775e7e8d251d5c0735bc	
Improper Locking	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: firmware: qcom: scm: Mark get_wq_ctx() as atomic call Currently get_wq_ctx() is wrongly configured as a standard call. When two SMC calls are in sleep and one SMC wakes up, it calls get_wq_ctx() to resume the corresponding sleeping thread. But if get_wq_ctx() is interrupted, goes to sleep and another	https://git.kernel.org/stable/c/9960085a3a82c58d3323c1c20b991db6045063b0, https://git.kernel.org/stable/c/cdf7efe4b02aa93813db0bf1ca596ad298ab6b06, https://git.kernel.org/stable/c/e40115c33c0d79c940545b6b12112aace7acd9f5	O-LIN-LINU-190924/3470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMC call is waiting to be allocated a waitq context, it leads to a deadlock. To avoid this get_wq_ctx() must be an atomic call and can't be a standard SMC call. Hence mark get_wq_ctx() as a fast call. **CVE ID: CVE-2024-46692**		
NULL Pointer Dereference	13-Sep-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: soc: qcom: pmic_glink: Fix race during initialization As pointed out by Stephen Boyd it is possible that during initialization of the pmic_glink child drivers, the protection-domain notifiers fires, and the associated work is scheduled, before the client registration returns and as a result the local	https://git.kernel.org/stable/c/1efdbf5323c9360e05066049b97414405e94e087, https://git.kernel.org/stable/c/3568affcddd68743e25aa3ec1647d9b82797757b, https://git.kernel.org/stable/c/943b0e7cc646a624bb20a68080f8f1a4a55df41c	O-LIN-LINU-190924/3471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"client" pointer has been initialized. The outcome of this is a NULL pointer dereference as the "client" pointer is blindly dereferenced. Timeline provided by Stephen: CPU0 CPU1 ---- --- ucsi->client = NULL; devm_pmic_glink_register_client() client->pdr_notify(client->priv, pg->client_state) pmic_glink_ucsi_pdr_notify() schedule_work(&ucsi->register_work) <schedule away> pmic_glink_ucsi_register() ucsi_register()		

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
			pmic_glink_ucsi_read_version() pmic_glink_ucsi_read() pmic_glink_ucsi_read() pmic_glink_send(ucsi->client) <client is NULL BAD> ucsi->client = client // Too late! This code is identical across the altmode, battery manager and usci child drivers. Resolve this by splitting the allocation of the "client" object and the registration thereof into two operations. This only happens if the protection domain registry is populated at the time of registration, which by the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			introduction of commit '1ebcde047c54 ("soc: qcom: add pd-mapper implementation")' became much more likely. **CVE ID: CVE-2024-46693**		
Affected Version(s): From (including) 6.8 Up to (excluding) 6.10.5					
Improper Locking	04-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Fix deadlock during RTC update There is a deadlock when runtime suspend waits for the flush of RTC work, and the RTC work calls ufshcd_rpm_get_sync() to wait for runtime resume. Here is deadlock backtrace: kworker/0:1 D 4892.876354 10 10971 4859 0x4208060 0x8 10	https://git.kernel.org/stable/c/3911af778f208e5f49d43ce739332b91e26bc48e, https://git.kernel.org/stable/c/f13f1858a28c68b7fc0d72c2008d5c1f80d2e8d5	O-LIN-LINU-190924/3472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0 120 670730152367 ptr f0ffff80c2e40000 0 1 0x00000001 0x000000ff 0x000000ff 0x000000ff <ffffffee5e71ddb0> __switch_to+0x1a8 /0x2d4 <ffffffee5e71e604> __schedule+0x684/ 0xa98 <ffffffee5e71ea60> schedule+0x48/0x c8 <ffffffee5e725f78> schedule_timeout+ 0x48/0x170 <ffffffee5e71fb74> do_wait_for_comm on+0x108/0x1b0 <ffffffee5e71efe0> wait_for_completio n+0x44/0x60 <ffffffee5d6de968> __flush_work+0x39 c/0x424 <ffffffee5d6decc0> __cancel_work_sync +0xd8/0x208 <ffffffee5d6dee2c> cancel_delayed_wo rk_sync+0x14/0x2 8 <ffffffee5e2551b8> __ufshcd_wl_suspen d+0x19c/0x480		

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
			<ffffffee5e255fb8> ufshcd_wl_runtime_suspend+0x3c/0x1d4 <ffffffee5dffd80c> scsi_runtime_suspend+0x78/0xc8 <ffffffee5df93580> __rpm_callback+0x94/0x3e0 <ffffffee5df90b0c> rpm_suspend+0x2d4/0x65c <ffffffee5df91448> __pm_runtime_suspend+0x80/0x114 <ffffffee5dffd95c> scsi_runtime_idle+0x38/0x6c <ffffffee5df912f4> rpm_idle+0x264/0x338 <ffffffee5df90f14> __pm_runtime_idle+0x80/0x110 <ffffffee5e24ce44> ufshcd_rtc_work+0x128/0x1e4 <ffffffee5d6e3a40> process_one_work+0x26c/0x650 <ffffffee5d6e65c8> worker_thread+0x260/0x3d8 <ffffffee5d6edec8> kthread+0x110/0x134 <ffffffee5d616b18> ret_from_fork+0x10/0x20		

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
			Skip updating RTC if RPM state is not RPM_ACTIVE. **CVE ID: CVE-2024-44953**		
Affected Version(s): From (including) 6.8 Up to (excluding) 6.10.7					
Use After Free	04-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Free job before xe_exec_queue_put Free job depends on job->vm being valid, the last xe_exec_queue_put can destroy the VM. Prevent UAF by freeing job before xe_exec_queue_put. (cherry picked from commit 32a42c93b74c8ca6d0915ea3eba21bceff53042f) **CVE ID: CVE-2024-44978**	https://git.kernel.org/stable/c/98aa0330f200b9b8fb9e1298e006eda57a13351c, https://git.kernel.org/stable/c/9e7f30563677fbeff62d368d5d2a5ac7aaa9746a	O-LIN-LINU-190924/3473
Out-of-bounds Read	04-Sep-2024	7.1	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/497d370a644d95a9f04271aa92cb96d32e84c770, https://git.kern	O-LIN-LINU-190924/3474

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
			drm/v3d: Fix out-of-bounds read in `v3d_csd_job_run()` When enabling UBSAN on Raspberry Pi 5, we get the following warning: [387.894977] UBSAN: array-index-out-of-bounds in drivers/gpu/drm/v3d/v3d_sched.c:320:3 [387.903868] index 7 is out of range for type '__u32 [7]' [387.909692] CPU: 0 PID: 1207 Comm: kworker/u16:2 Tainted: G WC 6.10.3-v8-16k-numa #151 [387.919166] Hardware name: Raspberry Pi 5 Model B Rev 1.0 (DT) [387.925961] Workqueue: v3d_csd drm_sched_run_job_work [gpu_sched] [387.932525] Call trace:	el.org/stable/c/d656b82c4b30cf12715e6cd129d3df808fde24a7	

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
			[387.935296] dump_backtrace+0x170/0x1b8 [387.939403] show_stack+0x20/0x38 [387.942907] dump_stack_lvl+0x90/0xd0 [387.946785] dump_stack+0x18/0x28 [387.950301] __ubsan_handle_out_of_bounds+0x98/0xd0 [387.955383] v3d_csd_job_run+0x3a8/0x438 [v3d] [387.960707] drm_sched_run_job_work+0x520/0x6d0 [gpu_sched] [387.966862] process_one_work+0x62c/0xb48 [387.971296] worker_thread+0x468/0x5b0 [387.975317] kthread+0x1c4/0x1e0 [387.978818] ret_from_fork+0x10/0x20 [387.983014] ---[end trace]--- This happens because the UAPI		

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
			provides only seven configuration registers and we are reading the eighth position of this u32 array. Therefore, fix the out-of-bounds read in `v3d_csd_job_run()` by accessing only seven positions on the '__u32 [7]' array. The eighth register exists indeed on V3D 7.1, but it isn't currently used. That being so, let's guarantee that it remains unused and add a note that it could be set in a future patch. **CVE ID: CVE-2024-44993**		
Incomplete Cleanup	11-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: xhci: Check for xhci->interrupters being allocated in xhci_mem_clearup()	https://git.kernel.org/stable/c/770cacc75b0091ece17349195d72133912c1ca7c, https://git.kernel.org/stable/c/dcdb52d948f3a17ccd3fce757d	O-LIN-LINU-190924/3475

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
			If xhci_mem_init() fails, it calls into xhci_mem_cleanup() to mop up the damage. If it fails early enough, before xhci->interrupters is allocated but after xhci->max_interrupters has been set, which happens in most (all?) cases, things get uglier, as xhci_mem_cleanup() unconditionally derefences xhci->interrupters. With prejudice. Gate the interrupt freeing loop with a check on xhci->interrupters being non-NULL. Found while debugging a DMA allocation issue that led the XHCI driver on this exact path. **CVE ID: CVE-2024-45027**	9bd981d7c32039	
Affected Version(s): From (including) 6.9 Up to (excluding) 6.10.7					

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
Out-of-bounds Write	11-Sep-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: md/raid1: Fix data corruption for degraded array with slow disk read_balance() will avoid reading from slow disks as much as possible, however, if valid data only lands in slow disks, and a new normal disk is still in recovery, unrecovered data can be read: raid1_read_request read_balance raid1_should_read_first -> return false choose_best_rdev -> normal disk is not recovered, return -1 choose_bb_rdev -> missing the checking of recovery, return the normal disk	https://git.kernel.org/stable/c/2febf5fdbf5d9a52ddc3e986971c8609b1582d67, https://git.kernel.org/stable/c/c916ca35308d3187c9928664f9be249b22a3a701	O-LIN-LINU-190924/3476

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
			-> read unrecovered data Root cause is that the checking of recovery is missing in choose_bb_rdev(). Hence add such checking to fix the problem. Also fix similar problem in choose_slow_rdev( ). **CVE ID: CVE-2024-45023**		
Affected Version(s): From (including) 6.9 Up to (excluding) 6.10.8					
Use After Free	13-Sep-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix potential UAF in nfsd4_cb_getattr_release Once we drop the delegation reference, the fields embedded in it are no longer safe to access. Do that last. **CVE ID: CVE-2024-46696**	https://git.kernel.org/stable/c/1116e0e372eb16dd907ec571ce5d4af325c55c10, https://git.kernel.org/stable/c/e0b66698a5ae41078f7490e8b3527013f5fccd6c	O-LIN-LINU-190924/3477

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
NULL Pointer Dereference	13-Sep-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nfsd: prevent panic for nfsv4.0 closed files in nfs4_show_open Prior to commit 3f29cc82a84c ("nfsd: split sc_status out of sc_type") states_show() relied on sc_type field to be of valid type before calling into a subfunction to show content of a particular stateid. From that commit, we split the validity of the stateid into sc_status and no longer changed sc_type to 0 while unhashing the stateid. This resulted in kernel oopsing for nfsv4.0 opens that stay around and in nfs4_show_open() would derefence sc_file which was NULL.	https://git.kernel.org/stable/c/a204501e1743d695ca2930ed25a2be9f8ced96d3, https://git.kernel.org/stable/c/ba0b697de298285301c71c258598226e06494236	O-LIN-LINU-190924/3478

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
			Instead, for closed open stateids forgo displaying information that relies of having a valid sc_file. To reproduce: mount the server with 4.0, read and close a file and then on the server cat /proc/fs/nfsd/clients/2/states [513.590804] Call trace: [513.590925] _raw_spin_lock+0xcc/0x160 [513.591119] nfs4_show_open+0x78/0x2c0 [nfsd] [513.591412] states_show+0x44c/0x488 [nfsd] [513.591681] seq_read_iter+0x5d8/0x760 [513.591896] seq_read+0x188/0x208 [513.592075] vfs_read+0x148/0x470		

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
			[513.592241] ksys_read+0xcc/0x178 **CVE ID: CVE-2024-46682**		
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
N/A	11-Sep-2024	7.8	The Samsung Universal Print Driver for Windows is potentially vulnerable to escalation of privilege allowing the creation of a reverse shell in the tool. This is only applicable for products in the application released or manufactured before 2018. **CVE ID: CVE-2024-5760**	N/A	O-MIC-WIND-190924/3479
Out-of-bounds Write	13-Sep-2024	7.8	Media Encoder versions 24.5, 23.6.8 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	O-MIC-WIND-190924/3480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID: CVE-2024-39377**		
Out-of-bounds Read	13-Sep-2024	7.8	Media Encoder versions 24.5, 23.6.8 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2024-41871**	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	O-MIC-WIND-190924/3481
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Sep-2024	7.8	After Effects versions 23.6.6, 24.5 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	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	O-MIC-WIND-190924/3482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-39380**		
Out-of-bounds Write	13-Sep-2024	7.8	After Effects versions 23.6.6, 24.5 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-2024-39381**	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	O-MIC-WIND-190924/3483
Out-of-bounds Write	13-Sep-2024	7.8	Premiere Pro versions 24.5, 23.6.8 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-2024-39384**	https://helpx.adobe.com/security/products/premiere_pro/apsb24-58.html	O-MIC-WIND-190924/3484

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 Underflow (Wrap or Wraparound)	13-Sep-2024	7.8	Illustrator versions 28.6, 27.9.5 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-2024-41857**	https://helpx.adobe.com/security/products/illustrator/apsb24-66.html	O-MIC-WIND-190924/3485
Out-of-bounds Write	13-Sep-2024	7.8	After Effects versions 23.6.6, 24.5 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-2024-41859**	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	O-MIC-WIND-190924/3486
Use After Free	13-Sep-2024	7.8	Illustrator versions 28.6, 27.9.5 and earlier are affected by a Use After Free vulnerability that could result in	https://helpx.adobe.com/security/products/illustrator/apsb24-66.html	O-MIC-WIND-190924/3487

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
			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-2024-43758**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Sep-2024	7.8	Photoshop Desktop versions 24.7.4, 25.11 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-2024-43756**	https://helpx.adobe.com/security/products/photoshop/apsb24-72.html	O-MIC-WIND-190924/3488
Out-of-bounds Write	13-Sep-2024	7.8	Photoshop Desktop versions 24.7.4, 25.11 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	https://helpx.adobe.com/security/products/photoshop/apsb24-72.html	O-MIC-WIND-190924/3489

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
			interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-43760**		
Out-of-bounds Write	13-Sep-2024	7.8	Photoshop Desktop versions 24.7.4, 25.11 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-2024-45108**	https://helpx.adobe.com/security/products/photoshop/apsb24-72.html	O-MIC-WIND-190924/3490
Out-of-bounds Write	13-Sep-2024	7.8	Photoshop Desktop versions 24.7.4, 25.11 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-2024-45109**	https://helpx.adobe.com/security/products/photoshop/apsb24-72.html	O-MIC-WIND-190924/3491

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
Use After Free	05-Sep-2024	5.5	Acrobat Reader versions 20.005.30636, 24.002.20964, 24.001.30123, 24.002.20991 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID: CVE-2024-45107**	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html	O-MIC-WIND-190924/3492
Out-of-bounds Read	13-Sep-2024	5.5	Media Encoder versions 24.5, 23.6.8 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	O-MIC-WIND-190924/3493

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
			CVE ID: CVE-2024-41870		
Out-of-bounds Read	13-Sep-2024	5.5	Media Encoder versions 24.5, 23.6.8 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-2024-41872**	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	O-MIC-WIND-190924/3494
Out-of-bounds Read	13-Sep-2024	5.5	Media Encoder versions 24.5, 23.6.8 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/media-encoder/apsb24-53.html	O-MIC-WIND-190924/3495

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
			CVE ID: CVE-2024-41873		
Out-of-bounds Read	13-Sep-2024	5.5	After Effects versions 23.6.6, 24.5 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-2024-39382**	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	O-MIC-WIND-190924/3496
Use After Free	13-Sep-2024	5.5	Premiere Pro versions 24.5, 23.6.8 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/premiere_pro/apsb24-58.html	O-MIC-WIND-190924/3497

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
			CVE ID: CVE-2024-39385		
Out-of-bounds Read	13-Sep-2024	5.5	After Effects versions 23.6.6, 24.5 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-2024-41867**	https://helpx.adobe.com/security/products/after_effects/apsb24-55.html	O-MIC-WIND-190924/3498
NULL Pointer Dereference	13-Sep-2024	5.5	Illustrator versions 28.6, 27.9.5 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a DoS condition. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/illustrator/apsb24-66.html	O-MIC-WIND-190924/3499

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
			victim must open a malicious file. **CVE ID: CVE-2024-43759**		
Out-of-bounds Read	13-Sep-2024	5.5	Illustrator versions 28.6, 27.9.5 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-2024-45111**	https://helpx.adobe.com/security/products/illustrator/apsb24-66.html	O-MIC-WIND-190924/3500
Product: windows_10_1507					
Affected Version(s): * Up to (excluding) 10.0.10240.20766					
N/A	10-Sep-2024	9.8	Microsoft is aware of a vulnerability in Servicing Stack that has rolled back the fixes for some vulnerabilities affecting Optional Components on Windows 10, version 1507 (initial version released July 2015). This means that an attacker could exploit these	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43491	O-MIC-WIND-190924/3501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			previously mitigated vulnerabilities on Windows 10, version 1507 (Windows 10 Enterprise 2015 LTSB and Windows 10 IoT Enterprise 2015 LTSB) systems that have installed the Windows security update released on March 12, 2024—KB5035858 (OS Build 10240.20526) or other updates released until August 2024. All later versions of Windows 10 are not impacted by this vulnerability. This servicing stack vulnerability is addressed by installing the September 2024 Servicing stack update (SSU KB5043936) AND the September 2024 Windows security update (KB5043083), in that order. Note: Windows 10, version 1507 reached the end of support (EOS) on May 9, 2017 for		

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
			devices running the Pro, Home, Enterprise, Education, and Enterprise IoT editions. Only Windows 10 Enterprise 2015 LTSB and Windows 10 IoT Enterprise 2015 LTSB editions are still under support. **CVE ID: CVE-2024-43491**		
N/A	10-Sep-2024	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38014**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014	O-MIC-WIND-190924/3502
N/A	10-Sep-2024	6.2	Windows Authentication Information Disclosure Vulnerability **CVE ID: CVE-2024-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38254	O-MIC-WIND-190924/3503
N/A	10-Sep-2024	5.5	Windows Kernel-Mode Driver Information Disclosure Vulnerability **CVE ID: CVE-2024-38256**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38256	O-MIC-WIND-190924/3504
N/A	10-Sep-2024	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217	O-MIC-WIND-190924/3505

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 10.0.10240.20766					
N/A	10-Sep-2024	9.8	Microsoft is aware of a vulnerability in Servicing Stack that has rolled back the fixes for some vulnerabilities affecting Optional Components on Windows 10, version 1507 (initial version released July 2015). This means that an attacker could exploit these previously mitigated vulnerabilities on Windows 10, version 1507 (Windows 10 Enterprise 2015 LTSB and Windows 10 IoT Enterprise 2015 LTSB) systems that have installed the Windows security update released on March 12, 2024—KB5035858 (OS Build 10240.20526) or other updates released until August 2024. All later versions of Windows 10 are not impacted by this vulnerability. This servicing stack vulnerability is	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43491	O-MIC-WIND-190924/3506

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
			addressed by installing the September 2024 Servicing stack update (SSU KB5043936) AND the September 2024 Windows security update (KB5043083), in that order. Note: Windows 10, version 1507 reached the end of support (EOS) on May 9, 2017 for devices running the Pro, Home, Enterprise, Education, and Enterprise IoT editions. Only Windows 10 Enterprise 2015 LTSB and Windows 10 IoT Enterprise 2015 LTSB editions are still under support. **CVE ID: CVE-2024-43491**		
Product: windows_10_1607					
Affected Version(s): * Up to (excluding) 10.0.14393.7336					
N/A	10-Sep-2024	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38014**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014	O-MIC-WIND-190924/3507
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-190924/3508

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
			Privilege Vulnerability **CVE ID: CVE-2024-38252**	guide/vulnerability/CVE-2024-38252	
N/A	10-Sep-2024	7.5	Microsoft AllJoyn API Information Disclosure Vulnerability **CVE ID: CVE-2024-38257**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38257	O-MIC-WIND-190924/3509
N/A	10-Sep-2024	6.2	Windows Authentication Information Disclosure Vulnerability **CVE ID: CVE-2024-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38254	O-MIC-WIND-190924/3510
N/A	10-Sep-2024	5.5	Windows Kernel-Mode Driver Information Disclosure Vulnerability **CVE ID: CVE-2024-38256**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38256	O-MIC-WIND-190924/3511
N/A	10-Sep-2024	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217	O-MIC-WIND-190924/3512
Product: windows_10_1809					
Affected Version(s): * Up to (excluding) 10.0.17763.6293					
N/A	10-Sep-2024	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38014**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014	O-MIC-WIND-190924/3513

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
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38252	O-MIC-WIND-190924/3514
N/A	10-Sep-2024	7.5	Microsoft AllJoyn API Information Disclosure Vulnerability **CVE ID: CVE-2024-38257**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38257	O-MIC-WIND-190924/3515
N/A	10-Sep-2024	6.2	Windows Authentication Information Disclosure Vulnerability **CVE ID: CVE-2024-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38254	O-MIC-WIND-190924/3516
N/A	10-Sep-2024	5.5	Windows Kernel-Mode Driver Information Disclosure Vulnerability **CVE ID: CVE-2024-38256**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38256	O-MIC-WIND-190924/3517
N/A	10-Sep-2024	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217	O-MIC-WIND-190924/3518
Product: windows_10_21h1					
Affected Version(s): * Up to (excluding) 10.0.19044.4894					
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-190924/3519

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
			CVE ID: CVE-2024-38252	lity/CVE-2024-38252	
N/A	10-Sep-2024	7.5	Microsoft AllJoyn API Information Disclosure Vulnerability **CVE ID: CVE-2024-38257**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38257	O-MIC-WIND-190924/3520
N/A	10-Sep-2024	6.2	Windows Authentication Information Disclosure Vulnerability **CVE ID: CVE-2024-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38254	O-MIC-WIND-190924/3521
N/A	10-Sep-2024	5.5	Windows Kernel-Mode Driver Information Disclosure Vulnerability **CVE ID: CVE-2024-38256**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38256	O-MIC-WIND-190924/3522
Product: windows_10_21h2					
Affected Version(s): * Up to (excluding) 10.0.19044.4894					
N/A	10-Sep-2024	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38014**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014	O-MIC-WIND-190924/3523
N/A	10-Sep-2024	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217	O-MIC-WIND-190924/3524
Product: windows_10_22h2					
Affected Version(s): * Up to (excluding) 10.0.19041.4894					

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
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38252	O-MIC-WIND-190924/3525
N/A	10-Sep-2024	7.5	Microsoft AllJoyn API Information Disclosure Vulnerability **CVE ID: CVE-2024-38257**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38257	O-MIC-WIND-190924/3526
N/A	10-Sep-2024	6.2	Windows Authentication Information Disclosure Vulnerability **CVE ID: CVE-2024-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38254	O-MIC-WIND-190924/3527
N/A	10-Sep-2024	5.5	Windows Kernel-Mode Driver Information Disclosure Vulnerability **CVE ID: CVE-2024-38256**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38256	O-MIC-WIND-190924/3528
Affected Version(s): * Up to (excluding) 10.0.19045.4894					
N/A	10-Sep-2024	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38014**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014	O-MIC-WIND-190924/3529
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38252	O-MIC-WIND-190924/3530

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
			CVE ID: CVE-2024-38252		
N/A	10-Sep-2024	7.5	Microsoft AllJoyn API Information Disclosure Vulnerability **CVE ID: CVE-2024-38257**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38257	O-MIC-WIND-190924/3531
N/A	10-Sep-2024	6.2	Windows Authentication Information Disclosure Vulnerability **CVE ID: CVE-2024-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38254	O-MIC-WIND-190924/3532
N/A	10-Sep-2024	5.5	Windows Kernel-Mode Driver Information Disclosure Vulnerability **CVE ID: CVE-2024-38256**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38256	O-MIC-WIND-190924/3533
N/A	10-Sep-2024	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217	O-MIC-WIND-190924/3534
Affected Version(s): * Up to (including) 10.0.19045.4894					
N/A	10-Sep-2024	6.2	Windows Authentication Information Disclosure Vulnerability **CVE ID: CVE-2024-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38254	O-MIC-WIND-190924/3535
Product: windows_11_21h2					
Affected Version(s): * Up to (excluding) 10.0.22000.3197					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Sep-2024	8.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-38259**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38259	O-MIC-WIND-190924/3536
N/A	10-Sep-2024	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38014**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014	O-MIC-WIND-190924/3537
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38252	O-MIC-WIND-190924/3538
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38253	O-MIC-WIND-190924/3539
N/A	10-Sep-2024	7.5	Microsoft AllJoyn API Information Disclosure Vulnerability **CVE ID: CVE-2024-38257**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38257	O-MIC-WIND-190924/3540
N/A	10-Sep-2024	6.2	Windows Authentication Information Disclosure Vulnerability **CVE ID: CVE-2024-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38254	O-MIC-WIND-190924/3541

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
N/A	10-Sep-2024	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217	O-MIC-WIND-190924/3542
Product: windows_11_22h2					
Affected Version(s): * Up to (excluding) 10.0.22621.4169					
N/A	10-Sep-2024	8.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-38259**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38259	O-MIC-WIND-190924/3543
N/A	10-Sep-2024	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38014**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014	O-MIC-WIND-190924/3544
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38252	O-MIC-WIND-190924/3545
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38253	O-MIC-WIND-190924/3546
N/A	10-Sep-2024	7.5	Microsoft AllJoyn API Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-190924/3547

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
			CVE ID: CVE-2024-38257	lity/CVE-2024-38257	
N/A	10-Sep-2024	6.2	Windows Authentication Information Disclosure Vulnerability **CVE ID: CVE-2024-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38254	O-MIC-WIND-190924/3548
N/A	10-Sep-2024	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217	O-MIC-WIND-190924/3549
Product: windows_11_23h2					
Affected Version(s): * Up to (excluding) 10.0.22621.4169					
N/A	10-Sep-2024	8.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-38259**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38259	O-MIC-WIND-190924/3550
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38252	O-MIC-WIND-190924/3551
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38253	O-MIC-WIND-190924/3552

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
N/A	10-Sep-2024	7.5	Microsoft AllJoyn API Information Disclosure Vulnerability **CVE ID: CVE-2024-38257**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38257	O-MIC-WIND-190924/3553
Affected Version(s): * Up to (excluding) 10.0.22631.4169					
N/A	10-Sep-2024	8.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-38259**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38259	O-MIC-WIND-190924/3554
N/A	10-Sep-2024	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38014**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014	O-MIC-WIND-190924/3555
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38252	O-MIC-WIND-190924/3556
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38253	O-MIC-WIND-190924/3557
N/A	10-Sep-2024	6.2	Windows Authentication Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38254	O-MIC-WIND-190924/3558

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
			CVE ID: CVE-2024-38254		
N/A	10-Sep-2024	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217	O-MIC-WIND-190924/3559
Product: windows_11_24h2					
Affected Version(s): * Up to (excluding) 10.0.26100.1742					
N/A	10-Sep-2024	8.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-38259**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38259	O-MIC-WIND-190924/3560
N/A	10-Sep-2024	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38014**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014	O-MIC-WIND-190924/3561
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38252	O-MIC-WIND-190924/3562
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38253	O-MIC-WIND-190924/3563
N/A	10-Sep-2024	6.2	Windows Authentication	https://msrc.microsoft.com/up	O-MIC-WIND-190924/3564

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
			Information Disclosure Vulnerability **CVE ID: CVE-2024-38254**	date-guide/vulnerability/CVE-2024-38254	
N/A	10-Sep-2024	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217	O-MIC-WIND-190924/3565
Affected Version(s): * Up to (including) 10.0.26100.1742					
N/A	10-Sep-2024	8.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-38259**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38259	O-MIC-WIND-190924/3566
Product: windows_server_2008					
Affected Version(s): -					
N/A	10-Sep-2024	9.8	Windows Remote Desktop Licensing Service Spoofing Vulnerability **CVE ID: CVE-2024-43455**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43455	O-MIC-WIND-190924/3567
N/A	10-Sep-2024	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38014**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014	O-MIC-WIND-190924/3568
N/A	10-Sep-2024	7.5	Windows Remote Desktop Licensing Service Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38258	O-MIC-WIND-190924/3569

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
			CVE ID: CVE-2024-38258		
N/A	10-Sep-2024	7.5	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38263**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38263	O-MIC-WIND-190924/3570
N/A	10-Sep-2024	7.3	Microsoft Windows Admin Center Information Disclosure Vulnerability **CVE ID: CVE-2024-43475**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43475	O-MIC-WIND-190924/3571
N/A	10-Sep-2024	7.1	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-43454**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43454	O-MIC-WIND-190924/3572
N/A	10-Sep-2024	5.5	Windows Kernel-Mode Driver Information Disclosure Vulnerability **CVE ID: CVE-2024-38256**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38256	O-MIC-WIND-190924/3573
N/A	10-Sep-2024	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217	O-MIC-WIND-190924/3574
Affected Version(s): r2					
N/A	10-Sep-2024	9.8	Windows Remote Desktop Licensing	https://msrc.microsoft.com/update-	O-MIC-WIND-190924/3575

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
			Service Spoofing Vulnerability **CVE ID: CVE-2024-43455**	guide/vulnerability/CVE-2024-43455	
N/A	10-Sep-2024	8.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38260**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38260	O-MIC-WIND-190924/3576
N/A	10-Sep-2024	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38014**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014	O-MIC-WIND-190924/3577
N/A	10-Sep-2024	7.5	Windows Remote Desktop Licensing Service Information Disclosure Vulnerability **CVE ID: CVE-2024-38258**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38258	O-MIC-WIND-190924/3578
N/A	10-Sep-2024	7.5	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38263**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38263	O-MIC-WIND-190924/3579
N/A	10-Sep-2024	7.1	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-43454**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43454	O-MIC-WIND-190924/3580

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
N/A	10-Sep-2024	5.5	Windows Kernel-Mode Driver Information Disclosure Vulnerability **CVE ID: CVE-2024-38256**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38256	O-MIC-WIND-190924/3581
N/A	10-Sep-2024	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217	O-MIC-WIND-190924/3582
Affected Version(s): sp2					
N/A	10-Sep-2024	7.1	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-43454**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43454	O-MIC-WIND-190924/3583
Product: windows_server_2012					
Affected Version(s): -					
N/A	10-Sep-2024	9.8	Windows Remote Desktop Licensing Service Spoofing Vulnerability **CVE ID: CVE-2024-43455**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43455	O-MIC-WIND-190924/3584
N/A	10-Sep-2024	8.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38260**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38260	O-MIC-WIND-190924/3585
N/A	10-Sep-2024	7.8	Windows Installer Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-190924/3586

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
			Privilege Vulnerability **CVE ID: CVE-2024-38014**	guide/vulnerability/CVE-2024-38014	
N/A	10-Sep-2024	7.5	Windows Remote Desktop Licensing Service Information Disclosure Vulnerability **CVE ID: CVE-2024-38258**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38258	O-MIC-WIND-190924/3587
N/A	10-Sep-2024	7.5	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38263**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38263	O-MIC-WIND-190924/3588
N/A	10-Sep-2024	7.1	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-43454**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43454	O-MIC-WIND-190924/3589
N/A	10-Sep-2024	5.5	Windows Kernel-Mode Driver Information Disclosure Vulnerability **CVE ID: CVE-2024-38256**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38256	O-MIC-WIND-190924/3590
N/A	10-Sep-2024	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217	O-MIC-WIND-190924/3591
Affected Version(s): r2					

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
N/A	10-Sep-2024	9.8	Windows Remote Desktop Licensing Service Spoofing Vulnerability **CVE ID: CVE-2024-43455**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43455	O-MIC-WIND-190924/3592
N/A	10-Sep-2024	8.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38260**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38260	O-MIC-WIND-190924/3593
N/A	10-Sep-2024	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38014**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014	O-MIC-WIND-190924/3594
N/A	10-Sep-2024	7.5	Windows Remote Desktop Licensing Service Information Disclosure Vulnerability **CVE ID: CVE-2024-38258**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38258	O-MIC-WIND-190924/3595
N/A	10-Sep-2024	7.5	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38263**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38263	O-MIC-WIND-190924/3596
N/A	10-Sep-2024	7.1	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43454	O-MIC-WIND-190924/3597

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
			CVE ID: CVE-2024-43454		
N/A	10-Sep-2024	5.5	Windows Kernel-Mode Driver Information Disclosure Vulnerability **CVE ID: CVE-2024-38256**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38256	O-MIC-WIND-190924/3598
N/A	10-Sep-2024	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217	O-MIC-WIND-190924/3599
Product: windows_server_2016					
Affected Version(s): * Up to (excluding) 10.0.14393.7336					
N/A	10-Sep-2024	9.8	Windows Remote Desktop Licensing Service Spoofing Vulnerability **CVE ID: CVE-2024-43455**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43455	O-MIC-WIND-190924/3600
N/A	10-Sep-2024	8.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38260**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38260	O-MIC-WIND-190924/3601
N/A	10-Sep-2024	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38014**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014	O-MIC-WIND-190924/3602
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-190924/3603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID: CVE-2024-38252**	guide/vulnerability/CVE-2024-38252	
N/A	10-Sep-2024	7.5	Microsoft AllJoyn API Information Disclosure Vulnerability **CVE ID: CVE-2024-38257**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38257	O-MIC-WIND-190924/3604
N/A	10-Sep-2024	7.5	Windows Remote Desktop Licensing Service Information Disclosure Vulnerability **CVE ID: CVE-2024-38258**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38258	O-MIC-WIND-190924/3605
N/A	10-Sep-2024	7.5	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38263**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38263	O-MIC-WIND-190924/3606
N/A	10-Sep-2024	7.1	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-43454**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43454	O-MIC-WIND-190924/3607
N/A	10-Sep-2024	6.2	Windows Authentication Information Disclosure Vulnerability **CVE ID: CVE-2024-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38254	O-MIC-WIND-190924/3608

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
N/A	10-Sep-2024	5.5	Windows Kernel-Mode Driver Information Disclosure Vulnerability **CVE ID: CVE-2024-38256**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38256	O-MIC-WIND-190924/3609
N/A	10-Sep-2024	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217	O-MIC-WIND-190924/3610
Affected Version(s): *					
N/A	10-Sep-2024	9.8	Windows Remote Desktop Licensing Service Spoofing Vulnerability **CVE ID: CVE-2024-43455**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43455	O-MIC-WIND-190924/3611
Product: windows_server_2019					
Affected Version(s): * Up to (excluding) 10.0.17763.6293					
N/A	10-Sep-2024	9.8	Windows Remote Desktop Licensing Service Spoofing Vulnerability **CVE ID: CVE-2024-43455**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43455	O-MIC-WIND-190924/3612
N/A	10-Sep-2024	8.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38260**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38260	O-MIC-WIND-190924/3613
N/A	10-Sep-2024	7.8	Windows Installer Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-190924/3614

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
			CVE ID: CVE-2024-38014	lity/CVE-2024-38014	
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38252	O-MIC-WIND-190924/3615
N/A	10-Sep-2024	7.5	Microsoft AllJoyn API Information Disclosure Vulnerability **CVE ID: CVE-2024-38257**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38257	O-MIC-WIND-190924/3616
N/A	10-Sep-2024	7.5	Windows Remote Desktop Licensing Service Information Disclosure Vulnerability **CVE ID: CVE-2024-38258**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38258	O-MIC-WIND-190924/3617
N/A	10-Sep-2024	7.5	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38263**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38263	O-MIC-WIND-190924/3618
N/A	10-Sep-2024	7.1	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-43454**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43454	O-MIC-WIND-190924/3619
N/A	10-Sep-2024	6.2	Windows Authentication Information	https://msrc.microsoft.com/update-	O-MIC-WIND-190924/3620

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
			Disclosure Vulnerability **CVE ID: CVE-2024-38254**	guide/vulnerability/CVE-2024-38254	
N/A	10-Sep-2024	5.5	Windows Kernel-Mode Driver Information Disclosure Vulnerability **CVE ID: CVE-2024-38256**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38256	O-MIC-WIND-190924/3621
N/A	10-Sep-2024	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217	O-MIC-WIND-190924/3622
Product: windows_server_2022					
Affected Version(s): * Up to (excluding) 10.0.20348.2700					
N/A	10-Sep-2024	9.8	Windows Remote Desktop Licensing Service Spoofing Vulnerability **CVE ID: CVE-2024-43455**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43455	O-MIC-WIND-190924/3623
N/A	10-Sep-2024	8.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-38259**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38259	O-MIC-WIND-190924/3624
N/A	10-Sep-2024	8.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38260**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38260	O-MIC-WIND-190924/3625

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
N/A	10-Sep-2024	7.8	Windows Installer Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38014**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014	O-MIC-WIND-190924/3626
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38252	O-MIC-WIND-190924/3627
N/A	10-Sep-2024	7.5	Microsoft AllJoyn API Information Disclosure Vulnerability **CVE ID: CVE-2024-38257**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38257	O-MIC-WIND-190924/3628
N/A	10-Sep-2024	7.5	Windows Remote Desktop Licensing Service Information Disclosure Vulnerability **CVE ID: CVE-2024-38258**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38258	O-MIC-WIND-190924/3629
N/A	10-Sep-2024	7.5	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38263**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38263	O-MIC-WIND-190924/3630
N/A	10-Sep-2024	7.1	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43454	O-MIC-WIND-190924/3631

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
			CVE ID: CVE-2024-43454		
N/A	10-Sep-2024	6.2	Windows Authentication Information Disclosure Vulnerability **CVE ID: CVE-2024-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38254	O-MIC-WIND-190924/3632
N/A	10-Sep-2024	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217	O-MIC-WIND-190924/3633
Product: windows_server_2022_23h2					
Affected Version(s): * Up to (excluding) 10.0.25398.1128					
N/A	10-Sep-2024	9.8	Windows Remote Desktop Licensing Service Spoofing Vulnerability **CVE ID: CVE-2024-43455**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43455	O-MIC-WIND-190924/3634
N/A	10-Sep-2024	8.8	Microsoft Management Console Remote Code Execution Vulnerability **CVE ID: CVE-2024-38259**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38259	O-MIC-WIND-190924/3635
N/A	10-Sep-2024	8.8	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38260**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38260	O-MIC-WIND-190924/3636
N/A	10-Sep-2024	7.8	Windows Installer Elevation of	https://msrc.microsoft.com/up	O-MIC-WIND-190924/3637

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
			Privilege Vulnerability **CVE ID: CVE-2024-38014**	date-guide/vulnerability/CVE-2024-38014	
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38252	O-MIC-WIND-190924/3638
N/A	10-Sep-2024	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability **CVE ID: CVE-2024-38253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38253	O-MIC-WIND-190924/3639
N/A	10-Sep-2024	7.5	Microsoft AllJoyn API Information Disclosure Vulnerability **CVE ID: CVE-2024-38257**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38257	O-MIC-WIND-190924/3640
N/A	10-Sep-2024	7.5	Windows Remote Desktop Licensing Service Information Disclosure Vulnerability **CVE ID: CVE-2024-38258**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38258	O-MIC-WIND-190924/3641
N/A	10-Sep-2024	7.5	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-38263**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38263	O-MIC-WIND-190924/3642

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
N/A	10-Sep-2024	7.1	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability **CVE ID: CVE-2024-43454**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43454	O-MIC-WIND-190924/3643
N/A	10-Sep-2024	6.2	Windows Authentication Information Disclosure Vulnerability **CVE ID: CVE-2024-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38254	O-MIC-WIND-190924/3644
N/A	10-Sep-2024	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability **CVE ID: CVE-2024-38217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217	O-MIC-WIND-190924/3645
Vendor: openatom					
Product: openharmony					
Affected Version(s): * Up to (including) 4.1.0					
Use After Free	02-Sep-2024	7.8	in OpenHarmony v4.1.0 and prior versions allow a local attacker cause the common permission is upgraded to root and sensitive information leak through use after free. **CVE ID: CVE-2024-41160**	N/A	O-OPE-OPEN-190924/3646
Affected Version(s): 4.0					

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
Out-of-bounds Read	02-Sep-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-2024-38382**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2024/2024-09.md	O-OPE-OPEN-190924/3647
Out-of-bounds Read	02-Sep-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-2024-39612**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2024/2024-09.md	O-OPE-OPEN-190924/3648
Affected Version(s): 4.0.1					
Out-of-bounds Read	02-Sep-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-2024-38382**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2024/2024-09.md	O-OPE-OPEN-190924/3649
Out-of-bounds Read	02-Sep-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-2024-39612**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2024/2024-09.md	O-OPE-OPEN-190924/3650
Affected Version(s): From (including) 4.0 Up to (including) 4.1					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	in OpenHarmony v4.1.0 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through out-of-bounds write. **CVE ID: CVE-2024-38386**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2024/2024-09.md	O-OPE-OPEN-190924/3651
Out-of-bounds Write	02-Sep-2024	7.8	in OpenHarmony v4.1.0 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through out-of-bounds write. **CVE ID: CVE-2024-39816**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2024/2024-09.md	O-OPE-OPEN-190924/3652
Use After Free	02-Sep-2024	7.8	in OpenHarmony v4.1.0 and prior versions allow a local attacker cause the common permission is upgraded to root and sensitive information leak through use after free. **CVE ID: CVE-2024-41157**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2024/2024-09.md	O-OPE-OPEN-190924/3653
Out-of-bounds Read	02-Sep-2024	7.5	in OpenHarmony v4.1.0 and prior versions allow a remote attacker cause information leak through out-of-bounds Read.	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2024/2024-09.md	O-OPE-OPEN-190924/3654

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
			CVE ID: CVE-2024-39775		
Integer Overflow or Wraparound	02-Sep-2024	5.5	in OpenHarmony v4.1.0 and prior versions allow a local attacker cause crash through integer overflow. **CVE ID: CVE-2024-28044**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2024/2024-09.md	O-OPE-OPEN-190924/3655
Vendor: openwrt					
Product: openwrt					
Affected Version(s): 19.07.0					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	O-OPE-OPEN-190924/3656
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/September-2024	O-OPE-OPEN-190924/3657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Affected Version(s): 21.02					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	O-OPE-OPEN-190924/3658
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204;	https://corp.mediatek.com/product-security-bulletin/September-2024	O-OPE-OPEN-190924/3659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**		
Affected Version(s): 22.03.5					
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944210; Issue ID: MSV-1561. **CVE ID: CVE-2024-20084**	https://corp.mediatek.com/product-security-bulletin/September-2024	O-OPE-OPEN-190924/3660
Out-of-bounds Read	02-Sep-2024	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08944204; Issue ID: MSV-1560. **CVE ID: CVE-2024-20085**	https://corp.mediatek.com/product-security-bulletin/September-2024	O-OPE-OPEN-190924/3661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Qnap					
Product: qts					
Affected Version(s): 4.5.4.1715					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QTS-190924/3662
Affected Version(s): 4.5.4.1723					
Improper Neutralization of Special Elements used in an OS Command	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QTS-190924/3663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**		
Affected Version(s): 4.5.4.1741					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QTS-190924/3664

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
			vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**		
Affected Version(s): 4.5.4.1787					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QTS-190924/3665
Affected Version(s): 4.5.4.1800					

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 Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QTS-190924/3666
Affected Version(s): 4.5.4.1892					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network.	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QTS-190924/3667

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
			QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**		
Affected Version(s): 4.5.4.1931					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QTS-190924/3668

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
			QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**		
Affected Version(s): 4.5.4.2012					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QTS-190924/3669
Affected Version(s): 4.5.4.2117					
Improper Neutralization of Special Elements	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QTS-190924/3670

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
used in an OS Command ('OS Command Injection')			operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**		
Affected Version(s): 4.5.4.2280					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected.	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QTS-190924/3671

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
			We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**		
Affected Version(s): 4.5.4.2374					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QTS-190924/3672

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
			CVE ID: CVE-2023-34974		
Affected Version(s): 4.5.4.2467					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QTS-190924/3673
Affected Version(s): 4.5.4.2627					
Improper Neutralization of Special Elements used in an OS Command ('OS	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QTS-190924/3674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**		
Affected Version(s): 5.1.0.2348					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3675

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3676
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QTS-190924/3677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3678

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3679
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QTS-190924/3680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3681

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3682
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): 5.1.0.2399					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3684

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3685
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QTS-190924/3686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3687

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3688
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QTS-190924/3689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3690

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3691
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): 5.1.0.2418					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3693

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3694
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QTS-190924/3695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3696

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3697
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QTS-190924/3698

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
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3699

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3700
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): 5.1.0.2444					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3702

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3703
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QTS-190924/3704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3705

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3706
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QTS-190924/3707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3708

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3709
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): 5.1.0.2466					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3711

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3712
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QTS-190924/3713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3714

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3715
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QTS-190924/3716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3717

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3718
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): 5.1.1.2491					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3720

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3721
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QTS-190924/3722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3723

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3724
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QTS-190924/3725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3726

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3727
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): 5.1.2.2533					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3729

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3730
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QTS-190924/3731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3732

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3733
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QTS-190924/3734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3735

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3736
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): 5.1.3.2578					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3738

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3739
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QTS-190924/3740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3741

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3742
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QTS-190924/3743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3744

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3745
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): 5.1.4.2596					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3747

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3748
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QTS-190924/3749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3750

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3751
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QTS-190924/3752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3753

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3754
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): 5.1.5.2645					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3756

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3757
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QTS-190924/3758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3759

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3760
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QTS-190924/3761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3762

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3763
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): 5.1.5.2679					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3765

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3766
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QTS-190924/3767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3768

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3769
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QTS-190924/3770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3771

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3772
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QTS-190924/3773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): 5.1.6.2722					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QTS-190924/3774

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
			QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QTS-190924/3775
Affected Version(s): 5.1.7.2770					
Improper Neutralization of Special Elements	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP	https://www.qnap.com/en/security-	O-QNA-QTS-190924/3776

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
used in a Command ('Command Injection')			operating system versions. If exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**	advisory/qsa-24-33	
Product: quts_hero					
Affected Version(s): h4.5.4.1771					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected.	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QUTS-190924/3777

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
			We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**		
Affected Version(s): h4.5.4.1800					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QUTS-190924/3778

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
			CVE ID: CVE-2023-34974		
Affected Version(s): h4.5.4.1813					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QUTS-190924/3779
Affected Version(s): h4.5.4.1848					
Improper Neutralization of Special Elements used in an OS Command ('OS	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QUTS-190924/3780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**		
Affected Version(s): h4.5.4.1892					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QUTS-190924/3781

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
			QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**		
Affected Version(s): h4.5.4.1951					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QUTS-190924/3782
Affected Version(s): h4.5.4.1971					
Improper Neutralizat	06-Sep-2024	8.8	An OS command injection	https://www.qnap.com/en/sec	O-QNA-QUTS-190924/3783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**	urity-advisory/qsa-24-32	
Affected Version(s): h4.5.4.1991					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network.	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QUTS-190924/3784

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
			QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**		
Affected Version(s): h4.5.4.2052					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QUTS-190924/3785

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
			QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**		
Affected Version(s): h4.5.4.2138					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QUTS-190924/3786
Affected Version(s): h4.5.4.2217					
Improper Neutralization of Special Elements	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QUTS-190924/3787

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
used in an OS Command ('OS Command Injection')			operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**		
Affected Version(s): h4.5.4.2272					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected.	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QUTS-190924/3788

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
			We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**		
Affected Version(s): h4.5.4.2374					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QUTS-190924/3789

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
			CVE ID: CVE-2023-34974		
Affected Version(s): h4.5.4.2476					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QUTS-190924/3790
Affected Version(s): h4.5.4.2626					
Improper Neutralization of Special Elements used in an OS Command ('OS	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could	https://www.qnap.com/en/security-advisory/qsa-24-32	O-QNA-QUTS-190924/3791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			allow users to execute commands via a network. QuTScloud, QVR, QES are not affected. We have already fixed the vulnerability in the following versions: QTS 4.5.4.2790 build 20240605 and later QuTS hero h4.5.4.2626 build 20231225 and later **CVE ID: CVE-2023-34974**		
Affected Version(s): h5.1.0.2409					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3792

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3793
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QUTS-190924/3794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3795

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3796
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QUTS-190924/3797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3798

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3799
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): h5.1.0.2424					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3801

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3802
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QUTS-190924/3803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3804

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3805
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QUTS-190924/3806

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
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3807

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3808
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3809

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
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): h5.1.0.2453					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3810

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3811
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QUTS-190924/3812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3813

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3814
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QUTS-190924/3815

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
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3816

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3817
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): h5.1.0.2466					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3819

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3820
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QUTS-190924/3821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3822

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3823
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QUTS-190924/3824

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
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3825

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3826
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3827

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
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): h5.1.1.2488					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3828

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3829
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QUTS-190924/3830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3831

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3832
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QUTS-190924/3833

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
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3834

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3835
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): h5.1.2.2534					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3837

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3838
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QUTS-190924/3839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3840

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3841
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QUTS-190924/3842

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
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3843

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3844
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3845

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
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): h5.1.3.2578					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3846

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3847
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QUTS-190924/3848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3849

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3850
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QUTS-190924/3851

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
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3852

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3853
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3854

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
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): h5.1.4.2596					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3855

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3856
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QUTS-190924/3857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3858

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3859
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QUTS-190924/3860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3861

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3862
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): h5.1.5.2647					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3864

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3865
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QUTS-190924/3866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3867

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3868
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QUTS-190924/3869

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
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3870

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3871
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): h5.1.5.2680					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Sep-2024	8.8	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3873

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51367**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Sep-2024	8.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21898**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3874
Improper Neutralization of Special Elements used in a Command	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QUTS-190924/3875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3876

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51366**		
NULL Pointer Dereference	06-Sep-2024	6.5	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to launch a denial-of-service (DoS) attack via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-51368**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3877
Improper Limitation of a Pathname to a Restricted	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QUTS-190924/3878

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
Directory ('Path Traversal')			exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3879

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
			QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21897**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-2024	4.8	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2023-50366**	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3880
Improper Neutralization of Special Elements used in a	06-Sep-2024	4.7	An OS command injection vulnerability has been reported to affect several QNAP operating system	https://www.qnap.com/en/security-advisory/qsa-24-20	O-QNA-QUTS-190924/3881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later **CVE ID: CVE-2024-21903**		
Affected Version(s): h5.1.6.2734					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QUTS-190924/3882

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
			QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Sep-2024	6.5	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770 build 20240520 and later **CVE ID: CVE-2024-21904**	https://www.qnap.com/en/security-advisory/qsa-24-23	O-QNA-QUTS-190924/3883
Affected Version(s): h5.1.7.2770					
Improper Neutralization of Special Elements	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP	https://www.qnap.com/en/security-	O-QNA-QUTS-190924/3884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			operating system versions. If exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**	advisory/qsa-24-33	
Affected Version(s): h5.1.7.2788					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QUTS-190924/3885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**		
Affected Version(s): h5.1.7.2794					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Sep-2024	7.8	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow local network users to execute commands via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later **CVE ID: CVE-2024-38641**	https://www.qnap.com/en/security-advisory/qsa-24-33	O-QNA-QUTS-190924/3886
Vendor: Qualcomm					
Product: 205_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 versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-205_-190924/3887
Product: 205_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-205_-190924/3888
Product: 215_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-215_-190924/3889
Product: 215_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-215_-190924/3890
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/security	O-QUA-215_-190924/3891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	bulletin/september-2024-bulletin.html	
Product: 315_5g_iot_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-315_-190924/3892
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-315_-190924/3893
Product: 9206_lte_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-9206-190924/3894
Product: apq8017_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-APQ8-190924/3895

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-APQ8-190924/3896
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-APQ8-190924/3897
Product: aqt1000_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-AQT1-190924/3898
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-AQT1-190924/3899
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-AQT1-190924/3900

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-AQT1-190924/3901
Product: ar8031_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-AR80-190924/3902
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-AR80-190924/3903
Product: ar8035_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-AR80-190924/3904
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-AR80-190924/3905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33060	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-AR80-190924/3906
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-AR80-190924/3907
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-AR80-190924/3908
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-AR80-190924/3909
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-AR80-190924/3910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33051	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-AR80-190924/3911
Product: ar9380_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-AR93-190924/3912
Product: c-v2x_9150_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-C-V2-190924/3913
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-C-V2-190924/3914

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
			CVE ID: CVE-2024-38401	bulletin/september-2024-bulletin.html	
Product: csr8811_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-CSR8-190924/3915
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-CSR8-190924/3916
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-CSR8-190924/3917
Product: csra6620_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-CSRA-190924/3918
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-CSRA-190924/3919
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-CSRA-190924/3920
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-CSRA-190924/3921
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-CSRA-190924/3922
Product: csra6640_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 versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-CSRA-190924/3923
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-CSRA-190924/3924
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-CSRA-190924/3925
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-CSRA-190924/3926
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-CSRA-190924/3927

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
Product: csrb31024_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-CSRB-190924/3928
Product: fastconnect_6200_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3929
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3930
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3931
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3932

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
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3933
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3934
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3935
Product: fastconnect_6700_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3936
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-FAST-190924/3937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33042	bulletin/september-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3938
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3939
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3940
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3941
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-FAST-190924/3942

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
			CVE ID: CVE-2024-33060	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3943
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3944
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3945
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3946
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-FAST-190924/3947

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
			information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: fastconnect_6800_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3948
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3949
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3950
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3951

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3952
Product: fastconnect_6900_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3953
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3954
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3955
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3957
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3958
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3959
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3960
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3961

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3962
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3963
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3964
Product: fastconnect_7800_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3965

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3966
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3967
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3968
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3969
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3970
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	O-QUA-FAST-190924/3971

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
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3972
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3973
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3974
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3975

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3976
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FAST-190924/3977
Product: flight_rb5_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FLIG-190924/3978
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FLIG-190924/3979
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-FLIG-190924/3980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38402	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FLIG-190924/3981
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FLIG-190924/3982
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FLIG-190924/3983
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FLIG-190924/3984
Product: fsm10055_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FSM1-190924/3985
Product: fsm10056_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FSM1-190924/3986
Product: fsm20055_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FSM2-190924/3987
Product: fsm20056_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-FSM2-190924/3988
Product: home_hub_100_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-HOME-190924/3989
Product: immersive_home_214_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IMME-190924/3990
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IMME-190924/3991
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IMME-190924/3992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: immersive_home_216_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IMME-190924/3993
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IMME-190924/3994
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IMME-190924/3995
Product: immersive_home_316_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-IMME-190924/3996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beacon/probe response frame. **CVE ID: CVE-2024-33048**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IMME-190924/3997
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IMME-190924/3998
Product: immersive_home_318_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IMME-190924/3999
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation	https://docs.qualcomm.com/product/publicresources/security	O-QUA-IMME-190924/4000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IMME-190924/4001
Product: immersive_home_3210_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IMME-190924/4002
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IMME-190924/4003
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-IMME-190924/4004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IMME-190924/4005
Product: immersive_home_326_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IMME-190924/4006
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IMME-190924/4007
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-IMME-190924/4008

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
			length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IMME-190924/4009
Product: ipq4018_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ4-190924/4010
Product: ipq4019_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ4-190924/4011

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
			CVE ID: CVE-2024-33050		
Product: ipq4028_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ4-190924/4012
Product: ipq4029_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ4-190924/4013
Product: ipq5010_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ5-190924/4014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ5-190924/4015
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ5-190924/4016
Product: ipq5028_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ5-190924/4017
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ5-190924/4018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ5-190924/4019
Product: ipq5300_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ5-190924/4020
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ5-190924/4021
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when	https://docs.qualcomm.com/product/publicresources/security	O-QUA-IPQ5-190924/4022

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
			common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	bulletin/september-2024-bulletin.html	
Product: ipq5302_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ5-190924/4023
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ5-190924/4024
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ5-190924/4025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq5312_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ5-190924/4026
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ5-190924/4027
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ5-190924/4028
Product: ipq5332_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-IPQ5-190924/4029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beacon/probe response frame. **CVE ID: CVE-2024-33048**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ5-190924/4030
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ5-190924/4031
Product: ipq6000_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ6-190924/4032
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation	https://docs.qualcomm.com/product/publicresources/security	O-QUA-IPQ6-190924/4033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ6-190924/4034
Product: ipq6010_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ6-190924/4035
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ6-190924/4036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ6-190924/4037
Product: ipq6018_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ6-190924/4038
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ6-190924/4039
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ6-190924/4040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: ipq6028_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ6-190924/4041
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ6-190924/4042
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ6-190924/4043
Product: ipq8064_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4044
Product: ipq8065_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4045
Product: ipq8068_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4046
Product: ipq8070a_firmware					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4047
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4048
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4049
Product: ipq8071a_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4050

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4051
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4052
Product: ipq8072a_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4053
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-IPQ8-190924/4054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4055
Product: ipq8074a_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4056
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4058
Product: ipq8076a_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4059
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4060
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: ipq8076_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4062
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4063
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4064
Product: ipq8078a_firmware					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4065
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4066
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4067
Product: ipq8078_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4068

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4069
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4070
Product: ipq8173_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4071
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-IPQ8-190924/4072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4073
Product: ipq8174_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4074
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ8-190924/4076
Product: ipq9008_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ9-190924/4077
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ9-190924/4078
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ9-190924/4079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: ipq9554_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ9-190924/4080
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ9-190924/4081
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ9-190924/4082
Product: ipq9570_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ9-190924/4083
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ9-190924/4084
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ9-190924/4085
Product: ipq9574_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ9-190924/4086

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ9-190924/4087
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ9-190924/4088
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-IPQ9-190924/4089
Product: mdm8215_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MDM8-190924/4090

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
Product: mdm9215_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MDM9-190924/4091
Product: mdm9250_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MDM9-190924/4092
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MDM9-190924/4093
Product: mdm9310_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MDM9-190924/4094
Product: mdm9615_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MDM9-190924/4095
Product: mdm9628_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MDM9-190924/4096
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MDM9-190924/4097
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MDM9-190924/4098
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MDM9-190924/4099

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MDM9-190924/4100
Product: mdm9640_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MDM9-190924/4101
Product: mdm9645_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MDM9-190924/4102
Product: mdm9650_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MDM9-190924/4103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MDM9-190924/4104
Product: msm8108_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MSM8-190924/4105
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MSM8-190924/4106
Product: msm8209_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MSM8-190924/4107
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MSM8-190924/4108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: msm8608_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MSM8-190924/4109
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MSM8-190924/4110
Product: msm8909w_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MSM8-190924/4111
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MSM8-190924/4112
Product: msm8996au_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-MSM8-190924/4113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33042	ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MSM8-190924/4114
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MSM8-190924/4115
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-MSM8-190924/4116
Product: qam8255p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4117
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4119
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4120
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4121
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4122
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4123

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4124
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4125
Product: qam8295p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4126
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4127
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QAM8-190924/4128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command control operations. **CVE ID: CVE-2024-33052**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4129
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4130
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4131
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4132
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QAM8-190924/4133

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
			common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	bulletin/september-2024-bulletin.html	
Product: qam8620p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4134
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4135
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4136
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4137

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4138
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4139
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4140
Product: qam8650p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4141
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and	https://docs.qualcomm.com/product/publicres	O-QUA-QAM8-190924/4142

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
			unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4143
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4144
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4145
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4147
Product: qam8775p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4148
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4149
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4150
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4151

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
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4152
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4153
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4154
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAM8-190924/4155
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QAM8-190924/4156

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
			information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: qamsrv1h_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAMS-190924/4157
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAMS-190924/4158
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAMS-190924/4159
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAMS-190924/4160

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAMS-190924/4161
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAMS-190924/4162
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAMS-190924/4163
Product: qamsrv1m_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAMS-190924/4164
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and	https://docs.qualcomm.com/product/publicres	O-QUA-QAMS-190924/4165

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
			unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAMS-190924/4166
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAMS-190924/4167
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAMS-190924/4168
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAMS-190924/4169

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QAMS-190924/4170
Product: qca0000_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA0-190924/4171
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA0-190924/4172
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA0-190924/4173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: qca1062_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA1-190924/4174
Product: qca1064_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA1-190924/4175
Product: qca2062_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA2-190924/4176
Product: qca2064_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCA2-190924/4177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33051	ber-2024-bulletin.html	
Product: qca2065_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA2-190924/4178
Product: qca2066_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA2-190924/4179
Product: qca4024_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA4-190924/4180
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA4-190924/4181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA4-190924/4182
Product: qca6174a_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4183
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4184
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4186
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4187
Product: qca6174_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4188
Product: qca6175a_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4189

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4190
Product: qca6310_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4191
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4192
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4193
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4194

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4195
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4196
Product: qca6320_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4197
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4198
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4200
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4201
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4202
Product: qca6335_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4203
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4205
Product: qca6391_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4206
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4207
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4208
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4209
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/pr	O-QUA-QCA6-190924/4210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4211
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4212
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4213
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4214

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
			CVE ID: CVE-2024-33057		
Product: qca6420_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4215
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4216
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4217
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4218
Product: qca6421_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCA6-190924/4219

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
			CVE ID: CVE-2024-33042	ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4220
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4221
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4222
Product: qca6426_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4223
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCA6-190924/4224

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
			CVE ID: CVE-2024-33052	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4225
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4226
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4227
Product: qca6430_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4228
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCA6-190924/4229

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
			CVE ID: CVE-2024-33052	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4230
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4231
Product: qca6431_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4232
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4233
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4235
Product: qca6436_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4236
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4237
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4238
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4239

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4240
Product: qca6554a_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4241
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4242
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4244
Product: qca6564au_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4245
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4246
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4247
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4248

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
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4249
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4250
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4251
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4252
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCA6-190924/4253

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
			information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: qca6564a_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4254
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4255
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4256
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4257
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	O-QUA-QCA6-190924/4258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4259
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4260
Product: qca6564_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4261
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4262
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	O-QUA-QCA6-190924/4263

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
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4264
Product: qca6574au_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4265
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4266
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4267
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCA6-190924/4268

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
			node simultaneously. **CVE ID: CVE-2024-33060**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4269
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4270
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4271
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4272
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element	https://docs.qualcomm.com/product/publicres	O-QUA-QCA6-190924/4273

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
			Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ources/security bulletin/september-2024-bulletin.html	
Product: qca6574a_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4274
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4275
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4276
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4277

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
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4278
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4279
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4280
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4281
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4282

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4283
Product: qca6574_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4284
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4285
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4286
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4287

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
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4288
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4289
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4290
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4291
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCA6-190924/4292

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
			information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: qca6584au_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4293
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4294
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4295
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4296
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-	https://docs.qualcomm.com/product/publicres	O-QUA-QCA6-190924/4297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4298
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4299
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4300
Product: qca6584_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCA6-190924/4301

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	bulletin/september-2024-bulletin.html	
Product: qca6595au_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4302
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4303
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4304
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4305
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCA6-190924/4306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38401	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4307
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4308
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4309
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4310
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCA6-190924/4311

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
			information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: qca6595_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4312
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4313
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4314
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4315
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	O-QUA-QCA6-190924/4316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4317
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4318
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4319
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4320

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
			CVE ID: CVE-2024-33057		
Product: qca6678aq_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4321
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4322
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4323
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4324
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCA6-190924/4325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4326
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4327
Product: qca6688aq_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4328
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4330
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4331
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4332
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4333
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCA6-190924/4334

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
			information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: qca6696_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4335
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4336
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4337
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4338
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	O-QUA-QCA6-190924/4339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4340
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4341
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4342
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4343
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element	https://docs.qualcomm.com/product/publicres	O-QUA-QCA6-190924/4344

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
			Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ources/security bulletin/september-2024-bulletin.html	
Product: qca6698aq_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4345
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4346
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4347
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4349
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4350
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4351
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4352
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4353

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4354
Product: qca6777aq_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4355
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4356
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: qca6787aq_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4358
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4359
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4360
Product: qca6797aq_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4361
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4362
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4363
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4364
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4365

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4366
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA6-190924/4367
Product: qca7500_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA7-190924/4368
Product: qca8075_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCA8-190924/4369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beacon/probe response frame. **CVE ID: CVE-2024-33048**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4370
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4371
Product: qca8081_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4372
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCA8-190924/4373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4374
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4375
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4376
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4377
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicres	O-QUA-QCA8-190924/4378

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4379
Product: qca8082_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4380
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4381
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCA8-190924/4382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	bulletin/september-2024-bulletin.html	
Product: qca8084_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4383
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4384
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca8085_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4386
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4387
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4388
Product: qca8337_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCA8-190924/4389

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
			CVE ID: CVE-2024-33045	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4390
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4391
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4392
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4393
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4394

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
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4395
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4396
Product: qca8386_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4397
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA8-190924/4399
Product: qca9367_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4400
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4401
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCA9-190924/4402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33051	ber-2024-bulletin.html	
Product: qca9377_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4403
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4404
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4405
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4406
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicres	O-QUA-QCA9-190924/4407

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	ources/security bulletin/september-2024-bulletin.html	
Product: qca9378_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4408
Product: qca9379_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4409
Product: qca9880_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4410
Product: qca9886_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4411
Product: qca9888_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4412
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4413
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: qca9889_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4415
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4416
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4417
Product: qca9898_firmware					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4418
Product: qca9980_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4419
Product: qca9984_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4420
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicres	O-QUA-QCA9-190924/4421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	ources/security bulletin/september-2024-bulletin.html	
Product: qca9985_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4422
Product: qca9990_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4423
Product: qca9992_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either missing or improper. **CVE ID: CVE-2024-33050**		
Product: qca9994_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCA9-190924/4425
Product: qcc2073_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCC2-190924/4426
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCC2-190924/4427

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCC2-190924/4428
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCC2-190924/4429
Product: qcc2076_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCC2-190924/4430
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCC2-190924/4431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCC2-190924/4432
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCC2-190924/4433
Product: qcc710_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCC7-190924/4434
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCC7-190924/4435
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCC7-190924/4436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38402	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCC7-190924/4437
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCC7-190924/4438
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCC7-190924/4439
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCC7-190924/4440
Product: qcf8000_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 versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCF8-190924/4441
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCF8-190924/4442
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCF8-190924/4443
Product: qcf8001_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCF8-190924/4444

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCF8-190924/4445
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCF8-190924/4446
Product: qcm2150_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM2-190924/4447
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM2-190924/4448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM2-190924/4449
Product: qcm2290_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM2-190924/4450
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM2-190924/4451
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM2-190924/4452
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM2-190924/4453
Product: qcm4290_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 versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4454
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4455
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4456
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4457
Product: qcm4325_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4458

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4459
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4460
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4461
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4462
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4463

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4464
Product: qcm4490_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4465
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4466
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4467
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4468
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and	https://docs.qualcomm.com/product/publicres	O-QUA-QCM4-190924/4469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4470
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4471
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM4-190924/4472
Product: qcm5430_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM5-190924/4473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM5-190924/4474
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM5-190924/4475
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM5-190924/4476
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM5-190924/4477
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM5-190924/4478
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	O-QUA-QCM5-190924/4479

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
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM5-190924/4480
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM5-190924/4481
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM5-190924/4482
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM5-190924/4483

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM5-190924/4484
Product: qcm6125_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM6-190924/4485
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM6-190924/4486
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM6-190924/4487
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM6-190924/4488

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
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM6-190924/4489
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM6-190924/4490
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM6-190924/4491
Product: qcm6490_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM6-190924/4492
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCM6-190924/4493

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
			CVE ID: CVE-2024-33042	bulletin/september-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM6-190924/4494
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM6-190924/4495
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM6-190924/4496
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM6-190924/4497
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCM6-190924/4498

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
			CVE ID: CVE-2024-33060	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM6-190924/4499
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM6-190924/4500
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM6-190924/4501
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM6-190924/4502
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCM6-190924/4503

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
			information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: qcm8550_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM8-190924/4504
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM8-190924/4505
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM8-190924/4506
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM8-190924/4507
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCM8-190924/4508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM8-190924/4509
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM8-190924/4510
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM8-190924/4511
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM8-190924/4512

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM8-190924/4513
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCM8-190924/4514
Product: qcn5022_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4515
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4517
Product: qcn5024_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4518
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4519
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: qcn5052_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4521
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4522
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4523
Product: qcn5122_firmware					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4524
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4525
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4526
Product: qcn5124_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4527

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4528
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4529
Product: qcn5152_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4530
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCN5-190924/4531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4532
Product: qcn5154_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4533
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4535
Product: qcn5164_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4536
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4537
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN5-190924/4538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: qcn6023_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4539
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4540
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4541
Product: qcn6024_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4542
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4543
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4544
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4545
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4546

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4547
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4548
Product: qcn6112_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4549
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4551
Product: qcn6122_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4552
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4553
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCN6-190924/4554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: qcn6132_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4555
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4556
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4557
Product: qcn6224_firmware					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4558
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4559
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4560
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4561
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4562

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4563
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4564
Product: qcn6274_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4565
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4566
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	O-QUA-QCN6-190924/4567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4568
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4569
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4570
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4571

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
			CVE ID: CVE-2024-33057		
Product: qcn6402_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4572
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4573
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4574
Product: qcn6412_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-	https://docs.qualcomm.com/product/publicres	O-QUA-QCN6-190924/4575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4576
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4577
Product: qcn6422_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4578

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4579
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4580
Product: qcn6432_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4581
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN6-190924/4583
Product: qcn7605_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN7-190924/4584
Product: qcn7606_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN7-190924/4585
Product: qcn9000_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCN9-190924/4586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4587
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4588
Product: qcn9011_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4589
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCN9-190924/4590

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
			node simultaneously. **CVE ID: CVE-2024-33060**	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4591
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4592
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4593
Product: qcn9012_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4594
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	O-QUA-QCN9-190924/4595

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
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4596
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4597
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4598
Product: qcn9022_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4599

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4600
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4601
Product: qcn9024_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4602
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4603

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
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4604
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4605
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4606
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4607
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCN9-190924/4608

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
			information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: qcn9070_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4609
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4610
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4611
Product: qcn9072_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 versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4612
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4613
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4614
Product: qcn9074_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4615

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
			CVE ID: CVE-2024-33060		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4616
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4617
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4618
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4619
Product: qcn9100_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 versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4620
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4621
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4622
Product: qcn9160_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4623

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4624
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4625
Product: qcn9274_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4626
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4628
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCN9-190924/4629
Product: qcs2290_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS2-190924/4630
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS2-190924/4631

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
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS2-190924/4632
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS2-190924/4633
Product: qcs410_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4634
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4635
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4636
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	O-QUA-QCS4-190924/4637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4638
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4639
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4640
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4641
Product: qcs4290_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4642
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4643
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4644
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4645
Product: qcs4490_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4646

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4647
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4648
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4649
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4650
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4651
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCS4-190924/4652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS4-190924/4653
Product: qcs5430_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS5-190924/4654
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS5-190924/4655
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS5-190924/4656
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCS5-190924/4657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invoked from user-space. **CVE ID: CVE-2024-33047**	bulletin/september-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS5-190924/4658
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS5-190924/4659
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS5-190924/4660
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS5-190924/4661
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCS5-190924/4662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beacon/probe response frame. **CVE ID: CVE-2024-33048**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS5-190924/4663
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS5-190924/4664
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS5-190924/4665
Product: qcs610_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCS6-190924/4666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33042	ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4667
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4668
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4669
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4670
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4671
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during	https://docs.qualcomm.com/product/publicres	O-QUA-QCS6-190924/4672

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
			new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4673
Product: qcs6125_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4674
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4675
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4676
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	O-QUA-QCS6-190924/4677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4678
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4679
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4680
Product: qcs6490_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4681

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4682
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4683
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4684
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4685
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4686
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	O-QUA-QCS6-190924/4687

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
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4688
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4689
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4690
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4691

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS6-190924/4692
Product: qcs7230_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS7-190924/4693
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS7-190924/4694
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS7-190924/4695
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS7-190924/4696

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
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS7-190924/4697
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS7-190924/4698
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS7-190924/4699
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS7-190924/4700
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QCS7-190924/4701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ber-2024-bulletin.html	
Product: qcs8250_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4702
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4703
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4704
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4705
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	O-QUA-QCS8-190924/4706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4707
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4708
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4709
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4710

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
			CVE ID: CVE-2024-33057		
Product: qcs8550_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4711
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4712
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4713
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4714
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33054		
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4716
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4717
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4718
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4719
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCS8-190924/4720

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QCS8-190924/4721
Product: qdu1000_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDU1-190924/4722
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDU1-190924/4723
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDU1-190924/4724
Product: qdu1010_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 versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDU1-190924/4725
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDU1-190924/4726
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDU1-190924/4727
Product: qdu1110_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDU1-190924/4728
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDU1-190924/4729

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
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDU1-190924/4730
Product: qdu1210_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDU1-190924/4731
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDU1-190924/4732
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDU1-190924/4733
Product: qdx1010_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDX1-190924/4734

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
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDX1-190924/4735
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDX1-190924/4736
Product: qdx1011_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDX1-190924/4737
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDX1-190924/4738
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QDX1-190924/4739
Product: qep8111_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 versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QEP8-190924/4740
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QEP8-190924/4741
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QEP8-190924/4742
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QEP8-190924/4743
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QEP8-190924/4744

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
Product: qfw7114_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QFW7-190924/4745
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QFW7-190924/4746
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QFW7-190924/4747
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QFW7-190924/4748
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QFW7-190924/4749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QFW7-190924/4750
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QFW7-190924/4751
Product: qfw7124_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QFW7-190924/4752
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QFW7-190924/4753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QFW7-190924/4754
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QFW7-190924/4755
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QFW7-190924/4756
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QFW7-190924/4757
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QFW7-190924/4758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: qrb5165m_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRB5-190924/4759
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRB5-190924/4760
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRB5-190924/4761
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRB5-190924/4762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRB5-190924/4763
Product: qrb5165n_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRB5-190924/4764
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRB5-190924/4765
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRB5-190924/4766
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRB5-190924/4767

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRB5-190924/4768
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRB5-190924/4769
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRB5-190924/4770
Product: qru1032_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRU1-190924/4771
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and	https://docs.qualcomm.com/product/publicres	O-QUA-QRU1-190924/4772

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
			unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRU1-190924/4773
Product: qru1052_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRU1-190924/4774
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRU1-190924/4775
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRU1-190924/4776
Product: qru1062_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRU1-190924/4777
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRU1-190924/4778
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QRU1-190924/4779
Product: qsm8250_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QSM8-190924/4780
Product: qsm8350_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QSM8-190924/4781

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
			CVE ID: CVE-2024-33045		
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QSM8-190924/4782
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QSM8-190924/4783
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QSM8-190924/4784
Product: qxm8083_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QXM8-190924/4785
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-QXM8-190924/4786

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
			frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-QXM8-190924/4787
Product: robotics_rb3_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-ROBO-190924/4788
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-ROBO-190924/4789
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-ROBO-190924/4790

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
Product: robotics_rb5_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-ROBO-190924/4791
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-ROBO-190924/4792
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-ROBO-190924/4793
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-ROBO-190924/4794
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-ROBO-190924/4795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-ROBO-190924/4796
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-ROBO-190924/4797
Product: sa4150p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA41-190924/4798
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA41-190924/4799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA41-190924/4800
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA41-190924/4801
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA41-190924/4802
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA41-190924/4803
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA41-190924/4804
Product: sa4155p_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 versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA41-190924/4805
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA41-190924/4806
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA41-190924/4807
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA41-190924/4808
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA41-190924/4809
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SA41-190924/4810

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
			in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA41-190924/4811
Product: sa6145p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4812
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4813
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4814
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and	https://docs.qualcomm.com/product/publicres	O-QUA-SA61-190924/4815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4816
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4817
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4818
Product: sa6150p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4819

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4820
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4821
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4822
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4823
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4824

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4825
Product: sa6155p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4826
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4827
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4828
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4829
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/pr	O-QUA-SA61-190924/4830

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
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4831
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4832
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4833
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33057		
Product: sa6155_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4835
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4836
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4837
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA61-190924/4838
Product: sa7255p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SA72-190924/4839

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
			messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA72-190924/4840
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA72-190924/4841
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA72-190924/4842
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA72-190924/4843

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA72-190924/4844
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA72-190924/4845
Product: sa7775p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA77-190924/4846
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA77-190924/4847
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SA77-190924/4848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38402	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA77-190924/4849
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA77-190924/4850
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA77-190924/4851
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA77-190924/4852
Product: sa8145p_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 versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4853
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4854
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4855
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4856
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4857
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SA81-190924/4858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4859
Product: sa8150p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4860
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4861
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4862
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and	https://docs.qualcomm.com/product/publicres	O-QUA-SA81-190924/4863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4864
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4865
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4866
Product: sa8155p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4867

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4868
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4869
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4870
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4871
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4872
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during	https://docs.qualcomm.com/product/publicres	O-QUA-SA81-190924/4873

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
			new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4874
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4875
Product: sa8155_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4876
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SA81-190924/4877

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
			CVE ID: CVE-2024-33052	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4878
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4879
Product: sa8195p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4880
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4881
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4882

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
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4883
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4884
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4885
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4886
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SA81-190924/4887

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
			CVE ID: CVE-2024-33051	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA81-190924/4888
Product: sa8255p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA82-190924/4889
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA82-190924/4890
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA82-190924/4891
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SA82-190924/4892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA82-190924/4893
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA82-190924/4894
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA82-190924/4895
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA82-190924/4896
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element	https://docs.qualcomm.com/product/publicres	O-QUA-SA82-190924/4897

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
			Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ources/security bulletin/september-2024-bulletin.html	
Product: sa8295p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA82-190924/4898
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA82-190924/4899
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA82-190924/4900
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA82-190924/4901

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
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA82-190924/4902
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA82-190924/4903
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA82-190924/4904
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA82-190924/4905
Product: sa8530p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new	https://docs.qualcomm.com/product/publicres	O-QUA-SA85-190924/4906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA85-190924/4907
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA85-190924/4908
Product: sa8540p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA85-190924/4909
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SA85-190924/4910

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
			length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA85-190924/4911
Product: sa8620p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA86-190924/4912
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA86-190924/4913
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA86-190924/4914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA86-190924/4915
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA86-190924/4916
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA86-190924/4917
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA86-190924/4918
Product: sa8650p_firmware					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA86-190924/4919
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA86-190924/4920
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA86-190924/4921
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA86-190924/4922
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA86-190924/4923

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA86-190924/4924
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA86-190924/4925
Product: sa8770p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA87-190924/4926
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA87-190924/4927
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SA87-190924/4928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command control operations. **CVE ID: CVE-2024-33052**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA87-190924/4929
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA87-190924/4930
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA87-190924/4931
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA87-190924/4932

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA87-190924/4933
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA87-190924/4934
Product: sa8775p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA87-190924/4935
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA87-190924/4936
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA87-190924/4937

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
			CVE ID: CVE-2024-33052		
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA87-190924/4938
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA87-190924/4939
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA87-190924/4940
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA87-190924/4941
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SA87-190924/4942

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA87-190924/4943
Product: sa9000p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA90-190924/4944
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA90-190924/4945
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA90-190924/4946
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	O-QUA-SA90-190924/4947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA90-190924/4948
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA90-190924/4949
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA90-190924/4950
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA90-190924/4951

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SA90-190924/4952
Product: sc8180x_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SC81-190924/4953
Product: sc8380xp_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SC83-190924/4954
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SC83-190924/4955
Product: sd460_firmware					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD46-190924/4956
Product: sd626_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD62-190924/4957
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD62-190924/4958
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD62-190924/4959
Product: sd660_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD66-190924/4960

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD66-190924/4961
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD66-190924/4962
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD66-190924/4963
Product: sd662_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD66-190924/4964
Product: sd670_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SD67-190924/4965

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
				ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD67-190924/4966
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD67-190924/4967
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD67-190924/4968
Product: sd675_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD67-190924/4969
Product: sd730_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SD73-190924/4970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33042	bulletin/september-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD73-190924/4971
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD73-190924/4972
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD73-190924/4973
Product: sd835_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD83-190924/4974
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SD83-190924/4975

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
			CVE ID: CVE-2024-33045	ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD83-190924/4976
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD83-190924/4977
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD83-190924/4978
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD83-190924/4979
Product: sd855_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SD85-190924/4980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33042	ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD85-190924/4981
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD85-190924/4982
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD85-190924/4983
Product: sd865_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD86-190924/4984
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD86-190924/4985

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
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD86-190924/4986
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD86-190924/4987
Product: sd888_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD88-190924/4988
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD88-190924/4989
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD88-190924/4990
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	O-QUA-SD88-190924/4991

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
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD88-190924/4992
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD88-190924/4993
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD88-190924/4994
Product: sdm429w_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDM4-190924/4995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDM4-190924/4996
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDM4-190924/4997
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDM4-190924/4998
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDM4-190924/4999
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDM4-190924/5000

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
			CVE ID: CVE-2024-33048		
Product: sdx20m_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDX2-190924/5001
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDX2-190924/5002
Product: sdx55_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDX5-190924/5003
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDX5-190924/5004
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SDX5-190924/5005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDX5-190924/5006
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDX5-190924/5007
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDX5-190924/5008
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDX5-190924/5009
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element	https://docs.qualcomm.com/product/publicres	O-QUA-SDX5-190924/5010

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
			Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ources/security bulletin/september-2024-bulletin.html	
Product: sdx61_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDX6-190924/5011
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDX6-190924/5012
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDX6-190924/5013
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDX6-190924/5014

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDX6-190924/5015
Product: sdx65m_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDX6-190924/5016
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDX6-190924/5017
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SDX6-190924/5018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33057		
Product: sd_455_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD_4-190924/5019
Product: sd_675_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD_6-190924/5020
Product: sd_8cx_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD_8-190924/5021
Product: sd_8_gen1_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD_8-190924/5022

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD_8-190924/5023
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD_8-190924/5024
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD_8-190924/5025
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD_8-190924/5026
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD_8-190924/5027
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SD_8-190924/5028

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
			frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SD_8-190924/5029
Product: sg4150p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SG41-190924/5030
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SG41-190924/5031
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SG41-190924/5032
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SG41-190924/5033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SG41-190924/5034
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SG41-190924/5035
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SG41-190924/5036
Product: sg8275p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SG82-190924/5037

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SG82-190924/5038
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SG82-190924/5039
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SG82-190924/5040
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SG82-190924/5041
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SG82-190924/5042

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SG82-190924/5043
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SG82-190924/5044
Product: sm4125_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM41-190924/5045
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM41-190924/5046
Product: sm4635_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 versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM46-190924/5047
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM46-190924/5048
Product: sm6250p_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM62-190924/5049
Product: sm6250_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM62-190924/5050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM62-190924/5051
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM62-190924/5052
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM62-190924/5053
Product: sm6370_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM63-190924/5054
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM63-190924/5055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM63-190924/5056
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM63-190924/5057
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM63-190924/5058
Product: sm7250p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM72-190924/5059
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM72-190924/5060

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
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM72-190924/5061
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM72-190924/5062
Product: sm7315_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM73-190924/5063
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM73-190924/5064
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM73-190924/5065
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	O-QUA-SM73-190924/5066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM73-190924/5067
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM73-190924/5068
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM73-190924/5069
Product: sm7325p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM73-190924/5070

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM73-190924/5071
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM73-190924/5072
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM73-190924/5073
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM73-190924/5074
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM73-190924/5075

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM73-190924/5076
Product: sm7435_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM74-190924/5077
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM74-190924/5078
Product: sm8550p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM85-190924/5079
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM85-190924/5080

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM85-190924/5081
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM85-190924/5082
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM85-190924/5083
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM85-190924/5084
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM85-190924/5085

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM85-190924/5086
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM85-190924/5087
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM85-190924/5088
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM85-190924/5089
Product: sm8635_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM86-190924/5090
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM86-190924/5091
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM86-190924/5092
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM86-190924/5093
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM86-190924/5094
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and	https://docs.qualcomm.com/product/publicres	O-QUA-SM86-190924/5095

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
			unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM86-190924/5096
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM86-190924/5097
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM86-190924/5098
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM86-190924/5099

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM86-190924/5100
Product: sm8750_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM87-190924/5101
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SM87-190924/5102
Product: smart_audio_200_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SMAR-190924/5103
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SMAR-190924/5104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command control operations. **CVE ID: CVE-2024-33052**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SMAR-190924/5105
Product: smart_audio_400_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SMAR-190924/5106
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SMAR-190924/5107
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SMAR-190924/5108
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SMAR-190924/5109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SMAR-190924/5110
Product: smart_display_200_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SMAR-190924/5111
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SMAR-190924/5112
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SMAR-190924/5113
Product: snapdragon_1200_wearable_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5114
Product: snapdragon_208_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5115
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5116
Product: snapdragon_210_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5117
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_212_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5119
Product: snapdragon_212_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5120
Product: snapdragon_425_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5121
Product: snapdragon_425_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5122
Product: snapdragon_429_firmware					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5123
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5124
Product: snapdragon_429_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5125
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5126
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5127

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
			CVE ID: CVE-2024-33060		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5128
Product: snapdragon_439_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5129
Product: snapdragon_439_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5130
Product: snapdragon_460_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5132
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5133
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5134
Product: snapdragon_460_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5135
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SNAP-190924/5136

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
			CVE ID: CVE-2024-33060	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5137
Product: snapdragon_480\+_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5138
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5139
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5140
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SNAP-190924/5141

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	ber-2024-bulletin.html	
Product: snapdragon_480\+_5g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5142
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5143
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5144
Product: snapdragon_480_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5145

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5146
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5147
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5148
Product: snapdragon_480_5g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5149
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SNAP-190924/5150

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
			CVE ID: CVE-2024-33060	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5151
Product: snapdragon_4_gen_1_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5152
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5153
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5154
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SNAP-190924/5155

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	ber-2024-bulletin.html	
Product: snapdragon_4_gen_1_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5156
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5157
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5158
Product: snapdragon_4_gen_2_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5160
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5161
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5162
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5163
Product: snapdragon_4_gen_2_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5164

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
			CVE ID: CVE-2024-33052		
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5165
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5166
Product: snapdragon_625_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5167
Product: snapdragon_625_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5168
Product: snapdragon_626_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5169
Product: snapdragon_626_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5170
Product: snapdragon_630_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5171
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5172
Product: snapdragon_630_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SNAP-190924/5173

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
			CVE ID: CVE-2024-33052	ber-2024-bulletin.html	
Product: snapdragon_632_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5174
Product: snapdragon_632_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5175
Product: snapdragon_636_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5176
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5177
Product: snapdragon_636_mobile_firmware					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5178
Product: snapdragon_660_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5179
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5180
Product: snapdragon_660_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5181
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5182

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
			CVE ID: CVE-2024-33060		
Product: snapdragon_662_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5183
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5184
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5185
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5186
Product: snapdragon_662_mobile_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5187
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5188
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5189
Product: snapdragon_665_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5190
Product: snapdragon_670_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5191

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5192
Product: snapdragon_670_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5193
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5194
Product: snapdragon_675_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5195
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5196

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
			CVE ID: CVE-2024-33051		
Product: snapdragon_675_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5197
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5198
Product: snapdragon_678_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5199
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5200
Product: snapdragon_678_mobile_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5201
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5202
Product: snapdragon_680_4g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5203
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5204
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5205

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5206
Product: snapdragon_680_4g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5207
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5208
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5209
Product: snapdragon_685_4g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SNAP-190924/5210

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
			CVE ID: CVE-2024-33042	ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5211
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5212
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5213
Product: snapdragon_685_4g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5214
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-190924/5215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5216
Product: snapdragon_690_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5217
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5218
Product: snapdragon_690_5g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5219
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-190924/5220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	bulletin/september-2024-bulletin.html	
Product: snapdragon_695_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5221
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5222
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5223
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5224
Product: snapdragon_695_5g_mobile_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5225
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5226
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5227
Product: snapdragon_6_gen_1_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5228
Product: snapdragon_6_gen_1_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SNAP-190924/5229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33052	ber-2024-bulletin.html	
Product: snapdragon_710_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5230
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5231
Product: snapdragon_710_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5232
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5233
Product: snapdragon_712_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5234
Product: snapdragon_720g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5235
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5236
Product: snapdragon_720g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5237
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5238

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
			CVE ID: CVE-2024-33060		
Product: snapdragon_730g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5239
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5240
Product: snapdragon_730g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5241
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5242
Product: snapdragon_730_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5243
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5244
Product: snapdragon_730_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5245
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5246
Product: snapdragon_732g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5247

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5248
Product: snapdragon_732g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5249
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5250
Product: snapdragon_750g_5g_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5251
Product: snapdragon_750g_5g_mobile_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-190924/5252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	bulletin/september-2024-bulletin.html	
Product: snapdragon_765g_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5253
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5254
Product: snapdragon_765g_5g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5255
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5256
Product: snapdragon_765_5g_firmware					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5257
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5258
Product: snapdragon_765_5g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5259
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5260
Product: snapdragon_768g_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5261

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5262
Product: snapdragon_768g_5g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5263
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5264
Product: snapdragon_778g\+_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5265
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5266

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
			CVE ID: CVE-2024-33045		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5267
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5268
Product: snapdragon_778g\+_5g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5269
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5270
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-190924/5271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	ources/security bulletin/september-2024-bulletin.html	
Product: snapdragon_778g_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5272
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5273
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5274
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5275
Product: snapdragon_778g_5g_mobile_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5276
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5277
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5278
Product: snapdragon_780g_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5279
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5281
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5282
Product: snapdragon_780g_5g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5283
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5284
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SNAP-190924/5285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38402	ber-2024-bulletin.html	
Product: snapdragon_782g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5286
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5287
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5288
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5289
Product: snapdragon_782g_mobile_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5290
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5291
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5292
Product: snapdragon_7c\+_gen_3_compute_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5293
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5294
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	O-QUA-SNAP-190924/5295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5296
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5297
Product: snapdragon_7c\+_gen_3_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5298
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5299
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-190924/5300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ources/security bulletin/september-2024-bulletin.html	
Product: snapdragon_7c_compute_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5301
Product: snapdragon_7c_gen_2_compute_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5302
Product: snapdragon_7\+_gen_2_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5303
Product: snapdragon_7\+_gen_2_mobile_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5304
Product: snapdragon_7_gen_1_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5305
Product: snapdragon_7_gen_1_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5306
Product: snapdragon_820_automotive_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5307
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SNAP-190924/5308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33052	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5309
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5310
Product: snapdragon_835_mobile_pc_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5311
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5312
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5313

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
			CVE ID: CVE-2024-33060		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5314
Product: snapdragon_835_pc_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5315
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5316
Product: snapdragon_845_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5317
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-190924/5318

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	bulletin/september-2024-bulletin.html	
Product: snapdragon_845_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5319
Product: snapdragon_850_compute_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5320
Product: snapdragon_855\+_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5321
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5322

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5323
Product: snapdragon_855\+_mobile_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5324
Product: snapdragon_855_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5325
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5326
Product: snapdragon_855_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-190924/5327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command control operations. **CVE ID: CVE-2024-33052**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5328
Product: snapdragon_860_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5329
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5330
Product: snapdragon_860_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5331
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	O-QUA-SNAP-190924/5332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Product: snapdragon_865\+_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5333
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5334
Product: snapdragon_865\+_5g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5335
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5336

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5337
Product: snapdragon_865_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5338
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5339
Product: snapdragon_865_5g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5340
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SNAP-190924/5341

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
			CVE ID: CVE-2024-33060	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5342
Product: snapdragon_870_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5343
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5344
Product: snapdragon_870_5g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5345
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-190924/5346

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
			node simultaneously. **CVE ID: CVE-2024-33060**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5347
Product: snapdragon_888\+_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5348
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5349
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5351
Product: snapdragon_888\+_5g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5352
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5353
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5354
Product: snapdragon_888_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5355

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5356
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5357
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5358
Product: snapdragon_888_5g_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5359
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SNAP-190924/5360

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
			CVE ID: CVE-2024-33060	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5361
Product: snapdragon_8cx_compute_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5362
Product: snapdragon_8cx_gen_2_5g_compute_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5363
Product: snapdragon_8cx_gen_3_compute_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5364
Product: snapdragon_8cx_gen_3_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5365
Product: snapdragon_8c_compute_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5366
Product: snapdragon_8\+_gen_1_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5367
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5368
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5369

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
			CVE ID: CVE-2024-33045		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5370
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5371
Product: snapdragon_8\+_gen_1_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5372
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5373
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-190924/5374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	ources/security bulletin/september-2024-bulletin.html	
Product: snapdragon_8\+_gen_2_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5375
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5376
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5377
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5379
Product: snapdragon_8\+_gen_2_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5380
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5381
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5382
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SNAP-190924/5383

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
				ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5384
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5385
Product: snapdragon_8_gen_1_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5386
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5388
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5389
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5390
Product: snapdragon_8_gen_1_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5391
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SNAP-190924/5392

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
			CVE ID: CVE-2024-33060	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5393
Product: snapdragon_8_gen_2_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5394
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5395
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5396
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5398
Product: snapdragon_8_gen_2_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5399
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5400
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5401
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/pr	O-QUA-SNAP-190924/5402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5403
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5404
Product: snapdragon_8_gen_3_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5405
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5406

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5407
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5408
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5409
Product: snapdragon_8_gen_3_mobile_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5410
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SNAP-190924/5411

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
			Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5412
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5413
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5414
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5415
Product: snapdragon_ar2_gen_1_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5416
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5417
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5418
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5419
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5420

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5421
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5422
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5423
Product: snapdragon_auto_4g_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5424

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5425
Product: snapdragon_auto_5g-rf_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5426
Product: snapdragon_auto_5g-rf_gen_2_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5427
Product: snapdragon_auto_5g_modem-rf_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5428
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SNAP-190924/5429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5430
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5431
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5432
Product: snapdragon_auto_5g_modem-rf_gen_2_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5433
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	O-QUA-SNAP-190924/5434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5435
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5436
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5437
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5438

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5439
Product: snapdragon_w5\+_gen_1_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5440
Product: snapdragon_w5\+_gen_1_wearable_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5441
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5442
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-190924/5443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5444
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5445
Product: snapdragon_wear_2100_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5446
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5447
Product: snapdragon_wear_2500_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 versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5448
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5449
Product: snapdragon_wear_3100_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5450
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5451
Product: snapdragon_x12_lte_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5452

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
			CVE ID: CVE-2024-33045		
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5453
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5454
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5455
Product: snapdragon_x20_lte_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5456
Product: snapdragon_x35_5g-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-190924/5457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	bulletin/september-2024-bulletin.html	
Product: snapdragon_x35_5g_modem-rf_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5458
Product: snapdragon_x35_5g_modem-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5459
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5460
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33050		
Product: snapdragon_x50_5g-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5462
Product: snapdragon_x50_5g_modem-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5463
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5464
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5465
Product: snapdragon_x55_5g-rf_system_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5466
Product: snapdragon_x55_5g_modem-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5467
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5468
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5469
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5470

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
Product: snapdragon_x5_lte_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5471
Product: snapdragon_x62_5g-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5472
Product: snapdragon_x62_5g_modem-rf_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5473
Product: snapdragon_x62_5g_modem-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5474
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-190924/5475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-190924/5476
Product: snapdragon_x65_5g-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5477
Product: snapdragon_x65_5g_modem-rf_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5478
Product: snapdragon_x65_5g_modem-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-200924/5479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	ources/security bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5480
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5481
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5482
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5483

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
			CVE ID: CVE-2024-33057		
Product: snapdragon_x72_5g-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5484
Product: snapdragon_x72_5g_modem-rf_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5485
Product: snapdragon_x72_5g_modem-rf_system_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5486
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5488
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5489
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5490
Product: snapdragon_x75_5g-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5491

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
Product: snapdragon_x75_5g_modem-rf_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5492
Product: snapdragon_x75_5g_modem-rf_system_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5493
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5494
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5495
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SNAP-200924/5496

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
			frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5497
Product: snapdragon_xr1_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5498
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5499
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5500

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
			CVE ID: CVE-2024-33060		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5501
Product: snapdragon_xr2\+_gen_1_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5502
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5503
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5504
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5505

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
Product: snapdragon_xr2_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5506
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5507
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5508
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SNAP-200924/5509
Product: srv1h_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5510

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
			CVE ID: CVE-2024-33045		
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5511
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5512
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5513
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5514
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SRV1-200924/5515

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5516
Product: srv1l_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5517
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5518
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5519

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5520
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5521
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5522
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5523
Product: srv1m_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5524
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5525
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5526
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5527
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5528

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5529
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SRV1-200924/5530
Product: ssg2115p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SSG2-200924/5531
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SSG2-200924/5532
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SSG2-200924/5533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SSG2-200924/5534
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SSG2-200924/5535
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SSG2-200924/5536
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SSG2-200924/5537
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element	https://docs.qualcomm.com/product/publicres	O-QUA-SSG2-200924/5538

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
			Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	ources/security bulletin/september-2024-bulletin.html	
Product: ssg2125p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SSG2-200924/5539
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SSG2-200924/5540
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SSG2-200924/5541
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SSG2-200924/5542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SSG2-200924/5543
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SSG2-200924/5544
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SSG2-200924/5545
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SSG2-200924/5546
Product: sw5100p_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SW51-200924/5547
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SW51-200924/5548
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SW51-200924/5549
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SW51-200924/5550
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SW51-200924/5551
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during	https://docs.qualcomm.com/product/publicres	O-QUA-SW51-200924/5552

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
			new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SW51-200924/5553
Product: sw5100_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SW51-200924/5554
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SW51-200924/5555
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SW51-200924/5556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SW51-200924/5557
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SW51-200924/5558
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SW51-200924/5559
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SW51-200924/5560
Product: sxr1120_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SXR1-200924/5561

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
			CVE ID: CVE-2024-33042	ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR1-200924/5562
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR1-200924/5563
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR1-200924/5564
Product: sxr1230p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR1-200924/5565
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR1-200924/5566

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
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR1-200924/5567
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR1-200924/5568
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR1-200924/5569
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR1-200924/5570
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SXR1-200924/5571

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
			CVE ID: CVE-2024-33051	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR1-200924/5572
Product: sxr2130_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5573
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5574
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5575
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicres	O-QUA-SXR2-200924/5576

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	ources/security bulletin/september-2024-bulletin.html	
Product: sxr2230p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5577
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5578
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5579
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5580
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-SXR2-200924/5581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38402	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5582
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5583
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5584
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5585
Product: sxr2250p_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5586
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5587
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5588
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5589
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5590
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SXR2-200924/5591

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
			element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5592
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5593
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-SXR2-200924/5594
Product: talynplus_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupt	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-TALY-200924/5595

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
			ed pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-TALY-200924/5596
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-TALY-200924/5597
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-TALY-200924/5598
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-TALY-200924/5599
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-TALY-200924/5600

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-TALY-200924/5601
Product: video_collaboration_vc1_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5602
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5603
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5604
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5605

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
			CVE ID: CVE-2024-33060		
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5606
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5607
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5608
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5609
Product: video_collaboration_vc3_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupt	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-VIDE-200924/5610

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
			ed pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5611
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5612
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5613
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5614
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5615

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
			CVE ID: CVE-2024-33054		
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5616
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5617
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5618
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5619
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5620

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
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5621
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5622
Product: video_collaboration_vc5_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5623
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5625
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5626
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5627
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5628
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5629

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
			CVE ID: CVE-2024-33050		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5630
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VIDE-200924/5631
Product: vision_intelligence_100_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VISI-200924/5632
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VISI-200924/5633
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single	https://docs.qualcomm.com/product/publicresources/security	O-QUA-VISI-200924/5634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node simultaneously. **CVE ID: CVE-2024-33060**	bulletin/september-2024-bulletin.html	
Product: vision_intelligence_200_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VISI-200924/5635
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VISI-200924/5636
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VISI-200924/5637
Product: vision_intelligence_300_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VISI-200924/5638
Product: vision_intelligence_400_firmware					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VISI-200924/5639
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VISI-200924/5640
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VISI-200924/5641
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VISI-200924/5642
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VISI-200924/5643

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VISI-200924/5644
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-VISI-200924/5645
Product: wcd9326_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5646
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5647
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5648

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
			CVE ID: CVE-2024-33060		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5649
Product: wcd9330_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5650
Product: wcd9335_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5651
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5652
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-WCD9-200924/5653

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
			CVE ID: CVE-2024-33052	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5654
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5655
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5656
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5657
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCD9-200924/5658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5659
Product: wcd9340_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5660
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5661
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5662
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	O-QUA-WCD9-200924/5663

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
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5664
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5665
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5666
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5667

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5668
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5669
Product: wcd9341_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5670
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5671
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5672

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
			CVE ID: CVE-2024-33052		
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5673
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5674
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5675
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5676
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5677

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
			either missing or improper. **CVE ID: CVE-2024-33050**		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5678
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5679
Product: wcd9360_firmware					
Affected Version(s): -					
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5680
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5682
Product: wcd9370_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5683
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5684
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5685
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5687
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5688
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5689
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5690
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5691

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5692
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5693
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5694
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5695
Product: wcd9371_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5696
Product: wcd9375_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5697
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5698
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5699
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5701
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5702
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5703
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5704
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5705

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5706
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5707
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5708
Product: wcd9378_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5709

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5710
Product: wcd9380_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5711
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5712
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5713
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5714

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
			CVE ID: CVE-2024-33047		
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5715
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5716
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5717
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5718
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5719

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
			CVE ID: CVE-2024-33048		
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5720
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5721
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5722
Product: wcd9385_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5723

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5724
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5725
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5726
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5727
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5728
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	O-QUA-WCD9-200924/5729

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
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5730
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5731
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5732
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5733

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5734
Product: wcd9390_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5735
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5736
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5737
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5738

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
			CVE ID: CVE-2024-33052		
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5739
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5740
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5741
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5742
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-WCD9-200924/5743

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
			frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5744
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5745
Product: wcd9395_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5746
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5748
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5749
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5750
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5751
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5752

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5753
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5754
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5755
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCD9-200924/5756
Product: wcn3610_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5757
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5758
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5759
Product: wcn3615_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5760
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5761
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and	https://docs.qualcomm.com/product/publicres	O-QUA-WCN3-200924/5762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5763
Product: wcn3620_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5764
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5765
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5766
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCN3-200924/5767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5768
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5769
Product: wcn3660b_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5770
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5771

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
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5772
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5773
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5774
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5775
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5776

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
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5777
Product: wcn3680b_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5778
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5779
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5780
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5781
Product: wcn3680_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5782
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5783
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5784
Product: wcn3910_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5785
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5786
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads	https://docs.qualcomm.com/pr	O-QUA-WCN3-200924/5787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5788
Product: wcn3950_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5789
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5790
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5791
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCN3-200924/5792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command control operations. **CVE ID: CVE-2024-33052**	bulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5793
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5794
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5795
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5796
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCN3-200924/5797

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
			frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	bulletin/september-2024-bulletin.html	
Product: wcn3980_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5798
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5799
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5800
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5801
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-WCN3-200924/5802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38401	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5803
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5804
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5805
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5806
Product: wcn3988_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5807
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5808
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5809
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5810
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5811
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-WCN3-200924/5812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38401	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5813
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5814
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5815
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5816
Product: wcn3990_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5817
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5818
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5819
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5820
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5821
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during	https://docs.qualcomm.com/product/publicres	O-QUA-WCN3-200924/5822

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
			new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ources/security bulletin/september-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5823
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5824
Product: wcn3999_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN3-200924/5825
Product: wcn6740_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN6-200924/5826
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN6-200924/5827
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN6-200924/5828
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN6-200924/5829
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN6-200924/5830
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-WCN6-200924/5831

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
			CVE ID: CVE-2024-38402	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN6-200924/5832
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN6-200924/5833
Product: wcn6755_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN6-200924/5834
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN6-200924/5835
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCN6-200924/5836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	bulletin/september-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN6-200924/5837
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN6-200924/5838
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN6-200924/5839
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN6-200924/5840
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-WCN6-200924/5841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beacon/probe response frame. **CVE ID: CVE-2024-33048**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN6-200924/5842
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN6-200924/5843
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WCN6-200924/5844
Product: wcn7880_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-WCN7-200924/5845

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
			CVE ID: CVE-2024-33051	ber-2024-bulletin.html	
Product: wsa8810_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5846
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5847
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5848
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5849
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5850

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
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5851
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5852
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5853
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5854
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5855

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
Product: wsa8815_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5856
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5857
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5858
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5859
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5860
Use After Free	02-Sep-2024	7.8	Memory corruption while processing	https://docs.qualcomm.com/pr	O-QUA-WSA8-200924/5861

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
			concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	oduct/publicresources/securitybulletin/september-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5862
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5863
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5864
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5865
Product: wsa8830_firmware					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5866
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5867
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5868
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5869
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5870
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-WSA8-200924/5871

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
			Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5872
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5873
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5874
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5875
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-WSA8-200924/5876

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
			frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5877
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5878
Product: wsa8832_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5879
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5881
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5882
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5883
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5884
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5886
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5887
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5888
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5889
Product: wsa8835_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5890
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5891
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5892
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5893
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5894
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-WSA8-200924/5895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	ber-2024-bulletin.html	
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5896
Use After Free	02-Sep-2024	7.8	Memory corruption while processing concurrent IOCTL calls. **CVE ID: CVE-2024-38401**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5897
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5898
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5899
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-WSA8-200924/5900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5901
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5902
Product: wsa8840_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5903
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5905
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5906
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5907
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5908
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5909

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
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5910
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5911
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5912
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5913
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5914

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
			before updating the location. **CVE ID: CVE-2024-33057**		
Product: wsa8845h_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5915
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5916
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5917
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5918
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations.	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-WSA8-200924/5919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33052	ber-2024-bulletin.html	
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5920
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5921
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5922
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5923
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe	https://docs.qualcomm.com/product/publicresources/securitybulletin/septem	O-QUA-WSA8-200924/5924

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
			frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	ber-2024-bulletin.html	
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5925
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing before updating the location. **CVE ID: CVE-2024-33057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5926
Product: wsa8845_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption while passing untrusted/corrupted pointers from DSP to EVA. **CVE ID: CVE-2024-33038**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5927
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when Alternative Frequency offset value is set to 255. **CVE ID: CVE-2024-33042**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when BTFM client sends new messages over Slimbus to ADSP. **CVE ID: CVE-2024-33045**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5929
Out-of-bounds Read	02-Sep-2024	7.8	Memory corruption when the captureRead QDCM command is invoked from user-space. **CVE ID: CVE-2024-33047**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5930
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption when user provides data for FM HCI command control operations. **CVE ID: CVE-2024-33052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5931
Out-of-bounds Write	02-Sep-2024	7.8	Memory corruption during the handshake between the Primary Virtual Machine and Trusted Virtual Machine. **CVE ID: CVE-2024-33054**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5932
Use After Free	02-Sep-2024	7.8	Memory corruption when two threads try to map and unmap a single node simultaneously. **CVE ID: CVE-2024-33060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5933

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
Use After Free	02-Sep-2024	7.8	Memory corruption while processing IOCTL call for getting group info. **CVE ID: CVE-2024-38402**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5934
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the received TID-to-link mapping element of beacon/probe response frame. **CVE ID: CVE-2024-33048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5935
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing MBSSID during new IE generation in beacon/probe frame when IE length check is either missing or improper. **CVE ID: CVE-2024-33050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5936
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while processing TIM IE from beacon frame as there is no check for IE length. **CVE ID: CVE-2024-33051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5937
Out-of-bounds Read	02-Sep-2024	7.5	Transient DOS while parsing the multi-link element Control field when common information length check is missing	https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2024-bulletin.html	O-QUA-WSA8-200924/5938

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
			before updating the location. **CVE ID: CVE-2024-33057**		
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 7.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	6.8	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. When buffers are partially filled with data, initialized parts of the buffer can be incorrectly accessed. **CVE ID: CVE-2024-45619**	https://access.redhat.com/security/cve/CVE-2024-45619, https://bugzilla.redhat.com/show_bug.cgi?id=2309288	O-RED-ENTE-200924/5939
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	6.8	A vulnerability was found in the pkcs15-init tool in OpenSC. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. When buffers are partially filled with data,	https://access.redhat.com/security/cve/CVE-2024-45620, https://bugzilla.redhat.com/show_bug.cgi?id=2309289	O-RED-ENTE-200924/5940

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
			initialized parts of the buffer can be incorrectly accessed. **CVE ID: CVE-2024-45620**		
Improper Enforcement of a Single, Unique Action	03-Sep-2024	6.5	A vulnerability was found in Keycloak. This flaw allows attackers to bypass brute force protection by exploiting the timing of login attempts. By initiating multiple login requests simultaneously, attackers can exceed the configured limits for failed attempts before the system locks them out. This timing loophole enables attackers to make more guesses at passwords than intended, potentially compromising account security on affected systems. **CVE ID: CVE-2024-4629**	https://access.redhat.com/errata/RHSA-2024:6493, https://access.redhat.com/errata/RHSA-2024:6494, https://access.redhat.com/errata/RHSA-2024:6495, https://access.redhat.com/errata/RHSA-2024:6497, https://access.redhat.com/errata/RHSA-2024:6499	O-RED-ENTE-200924/5941
Use of Uninitialized Resource	03-Sep-2024	3.9	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK.	https://access.redhat.com/security/cve/CVE-2024-45615, https://bugzilla.redhat.com/sh	O-RED-ENTE-200924/5942

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 problem is missing initialization of variables expected to be initialized (as arguments to other functions, etc.). **CVE ID: CVE-2024-45615**	ow_bug.cgi?id=2309285	
Use of Uninitialized Resource	03-Sep-2024	3.9	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. The following problems were caused by insufficient control of the response APDU buffer and its length when communicating with the card. **CVE ID: CVE-2024-45616**	https://access.redhat.com/security/cve/CVE-2024-45616, https://bugzilla.redhat.com/show_bug.cgi?id=2309290	O-RED-ENTE-200924/5943
Use of Uninitialized Resource	03-Sep-2024	3.9	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK. An attacker could use a crafted USB Device or	https://access.redhat.com/security/cve/CVE-2024-45617, https://bugzilla.redhat.com/show_bug.cgi?id=2309286	O-RED-ENTE-200924/5944

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
			Smart Card, which would present the system with a specially crafted response to APDUs. Insufficient or missing checking of return values of functions leads to unexpected work with variables that have not been initialized. **CVE ID: CVE-2024-45617**		
Use of Uninitialized Resource	03-Sep-2024	3.9	A vulnerability was found in pkcs15-init in OpenSC. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. Insufficient or missing checking of return values of functions leads to unexpected work with variables that have not been initialized. **CVE ID: CVE-2024-45618**	https://access.redhat.com/security/cve/CVE-2024-45618, https://bugzilla.redhat.com/show_bug.cgi?id=2309287	O-RED-ENTE-200924/5945
Affected Version(s): 8.0					
Buffer Copy	03-Sep-2024	6.8	A vulnerability was found in OpenSC,	https://access.redhat.com/secu	O-RED-ENTE-200924/5946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			OpenSC tools, PKCS#11 module, minidriver, and CTK. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. When buffers are partially filled with data, initialized parts of the buffer can be incorrectly accessed. **CVE ID: CVE-2024-45619**	rity/cve/CVE-2024-45619, https://bugzilla.redhat.com/show_bug.cgi?id=2309288	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	6.8	A vulnerability was found in the pkcs15-init tool in OpenSC. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. When buffers are partially filled with data, initialized parts of the buffer can be incorrectly accessed. **CVE ID: CVE-2024-45620**	https://access.redhat.com/security/cve/CVE-2024-45620, https://bugzilla.redhat.com/show_bug.cgi?id=2309289	O-RED-ENTE-200924/5947
Improper Enforcement of a Single,	03-Sep-2024	6.5	A vulnerability was found in Keycloak. This flaw allows attackers to bypass	https://access.redhat.com/errata/RHSA-2024:6493,	O-RED-ENTE-200924/5948

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
Unique Action			brute force protection by exploiting the timing of login attempts. By initiating multiple login requests simultaneously, attackers can exceed the configured limits for failed attempts before the system locks them out. This timing loophole enables attackers to make more guesses at passwords than intended, potentially compromising account security on affected systems. **CVE ID: CVE-2024-4629**	https://access.redhat.com/errata/RHSA-2024:6494, https://access.redhat.com/errata/RHSA-2024:6495, https://access.redhat.com/errata/RHSA-2024:6497, https://access.redhat.com/errata/RHSA-2024:6499	
Use of Uninitialized Resource	03-Sep-2024	3.9	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK. The problem is missing initialization of variables expected to be initialized (as arguments to other functions, etc.). **CVE ID: CVE-2024-45615**	https://access.redhat.com/security/cve/CVE-2024-45615, https://bugzilla.redhat.com/show_bug.cgi?id=2309285	O-RED-ENTE-200924/5949

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
Use of Uninitialized Resource	03-Sep-2024	3.9	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. The following problems were caused by insufficient control of the response APDU buffer and its length when communicating with the card. **CVE ID: CVE-2024-45616**	https://access.redhat.com/security/cve/CVE-2024-45616, https://bugzilla.redhat.com/show_bug.cgi?id=2309290	O-RED-ENTE-200924/5950
Use of Uninitialized Resource	03-Sep-2024	3.9	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. Insufficient or missing checking of return values of	https://access.redhat.com/security/cve/CVE-2024-45617, https://bugzilla.redhat.com/show_bug.cgi?id=2309286	O-RED-ENTE-200924/5951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functions leads to unexpected work with variables that have not been initialized. **CVE ID: CVE-2024-45617**		
Use of Uninitialized Resource	03-Sep-2024	3.9	A vulnerability was found in pkcs15-init in OpenSC. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. Insufficient or missing checking of return values of functions leads to unexpected work with variables that have not been initialized. **CVE ID: CVE-2024-45618**	https://access.redhat.com/security/cve/CVE-2024-45618, https://bugzilla.redhat.com/show_bug.cgi?id=2309287	O-RED-ENTE-200924/5952
Affected Version(s): 9.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	6.8	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted	https://access.redhat.com/security/cve/CVE-2024-45619, https://bugzilla.redhat.com/show_bug.cgi?id=2309288	O-RED-ENTE-200924/5953

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
			response to APDUs. When buffers are partially filled with data, initialized parts of the buffer can be incorrectly accessed. **CVE ID: CVE-2024-45619**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	6.8	A vulnerability was found in the pkcs15-init tool in OpenSC. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. When buffers are partially filled with data, initialized parts of the buffer can be incorrectly accessed. **CVE ID: CVE-2024-45620**	https://access.redhat.com/security/cve/CVE-2024-45620, https://bugzilla.redhat.com/show_bug.cgi?id=2309289	O-RED-ENTE-200924/5954
Improper Enforcement of a Single, Unique Action	03-Sep-2024	6.5	A vulnerability was found in Keycloak. This flaw allows attackers to bypass brute force protection by exploiting the timing of login attempts. By initiating multiple login requests simultaneously, attackers can exceed the	https://access.redhat.com/errata/RHSA-2024:6493, https://access.redhat.com/errata/RHSA-2024:6494, https://access.redhat.com/errata/RHSA-2024:6495, https://access.redhat.com/erra	O-RED-ENTE-200924/5955

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
			configured limits for failed attempts before the system locks them out. This timing loophole enables attackers to make more guesses at passwords than intended, potentially compromising account security on affected systems. **CVE ID: CVE-2024-4629**	ta/RHSA-2024:6497, https://access.redhat.com/errata/RHSA-2024:6499	
Use of Uninitialized Resource	03-Sep-2024	3.9	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK. The problem is missing initialization of variables expected to be initialized (as arguments to other functions, etc.). **CVE ID: CVE-2024-45615**	https://access.redhat.com/security/cve/CVE-2024-45615, https://bugzilla.redhat.com/show_bug.cgi?id=2309285	O-RED-ENTE-200924/5956
Use of Uninitialized Resource	03-Sep-2024	3.9	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK. An attacker could use a crafted USB Device or Smart Card, which would present the system with a	https://access.redhat.com/security/cve/CVE-2024-45616, https://bugzilla.redhat.com/show_bug.cgi?id=2309290	O-RED-ENTE-200924/5957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted response to APDUs. The following problems were caused by insufficient control of the response APDU buffer and its length when communicating with the card. **CVE ID: CVE-2024-45616**		
Use of Uninitialized Resource	03-Sep-2024	3.9	A vulnerability was found in OpenSC, OpenSC tools, PKCS#11 module, minidriver, and CTK. An attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. Insufficient or missing checking of return values of functions leads to unexpected work with variables that have not been initialized. **CVE ID: CVE-2024-45617**	https://access.redhat.com/security/cve/CVE-2024-45617, https://bugzilla.redhat.com/show_bug.cgi?id=2309286	O-RED-ENTE-200924/5958
Use of Uninitialized Resource	03-Sep-2024	3.9	A vulnerability was found in pkcs15-init in OpenSC. An	https://access.redhat.com/security/cve/CVE-	O-RED-ENTE-200924/5959

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
			attacker could use a crafted USB Device or Smart Card, which would present the system with a specially crafted response to APDUs. Insufficient or missing checking of return values of functions leads to unexpected work with variables that have not been initialized. **CVE ID: CVE-2024-45618**	2024-45618, https://bugzilla.redhat.com/show_bug.cgi?id=2309287	
Vendor: Samsung					
Product: android					
Affected Version(s): 14.0					
Improper Handling of Exceptional Conditions	04-Sep-2024	7.1	Improper handling of exceptional conditions in ThemeCenter prior to SMR Sep-2024 Release 1 allows local attackers to delete non-preloaded applications. **CVE ID: CVE-2024-34638**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5960
N/A	04-Sep-2024	5.5	Improper access control in WindowManagerService prior to SMR Sep-2024 Release 1 in Android 12, and SMR Jun-2024	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5961

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
			Release 1 in Android 13 and Android 14 allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34637**		
N/A	04-Sep-2024	5.5	Improper access control in key input related function in Dressroom prior to SMR Sep-2024 Release 1 allows local attackers to access protected data. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34643**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5962
N/A	04-Sep-2024	5.5	Improper access control in item selection related in Dressroom prior to SMR Sep-2024 Release 1 allows local attackers to access protected data. User interaction is required for triggering this vulnerability. **CVE ID: CVE-2024-34644**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5963
N/A	04-Sep-2024	5.5	Improper access control in	https://security.samsungmobile	O-SAM-ANDR-200924/5964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DualDarManagerProxy prior to SMR Sep-2024 Release 1 allows local attackers to cause local permanent denial of service. **CVE ID: CVE-2024-34646**	.com/securityUpdate.smsb?year=2024&month=09	
N/A	04-Sep-2024	5.5	Incorrect use of privileged API in DualDarManagerProxy prior to SMR Sep-2024 Release 1 allows local attackers to access privileged APIs related to knox without proper license. **CVE ID: CVE-2024-34647**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5965
Incorrect Default Permissions	04-Sep-2024	5.5	Improper Handling of Insufficient Permissions in KnoxMiscPolicy prior to SMR Sep-2024 Release 1 allows local attackers to access sensitive data. **CVE ID: CVE-2024-34648**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5966
Incorrect Authorization	04-Sep-2024	5.5	Improper authorization in My Files prior to SMR Sep-2024 Release 1 allows local attackers to access restricted data in My Files.	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5967

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
			CVE ID: CVE-2024-34651		
N/A	04-Sep-2024	5.5	Improper Export of android application component in My Files prior to SMR Sep-2024 Release 1 allows local attackers to access files with My Files' privilege. **CVE ID: CVE-2024-34654**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5968
N/A	04-Sep-2024	5.5	Incorrect use of privileged API in UniversalCredentialManager prior to SMR Sep-2024 Release 1 allows local attackers to access privileged API related to UniversalCredentialManager. **CVE ID: CVE-2024-34655**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5969
Improper Handling of Exceptional Conditions	04-Sep-2024	4.6	Improper handling of exceptional conditions in Setupwizard prior to SMR Aug-2024 Release 1 allows physical attackers to bypass proper validation. **CVE ID: CVE-2024-34639**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-200924/5970
Incorrect Authorization	04-Sep-2024	4.6	Improper authorization in One UI Home prior to SMR Sep-2024 Release 1 allows	https://security.samsungmobile.com/securityUpdate.smsb?yea	O-SAM-ANDR-200924/5971

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
			physical attackers to temporarily access sensitive information. **CVE ID: CVE-2024-34642**	r=2024&month=09	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Sep-2024	4.6	Path Traversal in My Files prior to SMR Sep-2024 Release 1 allows physical attackers to access directories with My Files' privilege. **CVE ID: CVE-2024-34653**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5972
N/A	04-Sep-2024	3.3	Improper access control vulnerability in BGProtectManager prior to SMR Sep-2024 Release 1 allows local attackers to bypass restriction of process expiration. **CVE ID: CVE-2024-34640**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5973
N/A	04-Sep-2024	3.3	Improper Export of Android Application Components in FeliCaTest prior to SMR Sep-2024 Release 1 allows local attackers to enable NFC configuration. **CVE ID: CVE-2024-34641**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5974

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
Incorrect Authorization	04-Sep-2024	3.3	Incorrect authorization in CocktailbarService prior to SMR Sep-2024 Release 1 allows local attackers to access privileged APIs related to Edge panel. **CVE ID: CVE-2024-34650**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5975
Incorrect Authorization	04-Sep-2024	3.3	Incorrect authorization in kperfmon prior to SMR Sep-2024 Release 1 allows local attackers to access information related to performance including app usage. **CVE ID: CVE-2024-34652**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5976
N/A	04-Sep-2024	2.4	Improper access control in new Dex Mode in multitasking framework prior to SMR Sep-2024 Release 1 allows physical attackers to temporarily access an unlocked screen. **CVE ID: CVE-2024-34649**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5977
Affected Version(s): 12.0					
Improper Handling of Exceptiona	04-Sep-2024	7.1	Improper handling of exceptional conditions in	https://security.samsungmobile.com/securityU	O-SAM-ANDR-200924/5978

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
l Conditions			ThemeCenter prior to SMR Sep-2024 Release 1 allows local attackers to delete non-preloaded applications. **CVE ID: CVE-2024-34638**	pdate.smsb?year=2024&month=09	
N/A	04-Sep-2024	5.5	Improper access control in WindowManagerService prior to SMR Sep-2024 Release 1 in Android 12, and SMR Jun-2024 Release 1 in Android 13 and Android 14 allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34637**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5979
N/A	04-Sep-2024	5.5	Improper access control in DualDarManagerProxy prior to SMR Sep-2024 Release 1 allows local attackers to cause local permanent denial of service. **CVE ID: CVE-2024-34646**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5980
N/A	04-Sep-2024	5.5	Incorrect use of privileged API in DualDarManagerProxy prior to SMR Sep-2024 Release 1	https://security.samsungmobile.com/securityUpdate.smsb?yea	O-SAM-ANDR-200924/5981

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
			allows local attackers to access privileged APIs related to knox without proper license. **CVE ID: CVE-2024-34647**	r=2024&month=09	
Incorrect Default Permissions	04-Sep-2024	5.5	Improper Handling of Insufficient Permissions in KnoxMiscPolicy prior to SMR Sep-2024 Release 1 allows local attackers to access sensitive data. **CVE ID: CVE-2024-34648**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5982
Incorrect Authorization	04-Sep-2024	5.5	Improper authorization in My Files prior to SMR Sep-2024 Release 1 allows local attackers to access restricted data in My Files. **CVE ID: CVE-2024-34651**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5983
N/A	04-Sep-2024	5.5	Incorrect use of privileged API in UniversalCredentialManager prior to SMR Sep-2024 Release 1 allows local attackers to access privileged API related to UniversalCredentialManager.	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5984

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
			CVE ID: CVE-2024-34655		
Improper Handling of Exceptional Conditions	04-Sep-2024	4.6	Improper handling of exceptional conditions in Setupwizard prior to SMR Aug-2024 Release 1 allows physical attackers to bypass proper validation. **CVE ID: CVE-2024-34639**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-200924/5985
Incorrect Authorization	04-Sep-2024	4.6	Improper authorization in One UI Home prior to SMR Sep-2024 Release 1 allows physical attackers to temporarily access sensitive information. **CVE ID: CVE-2024-34642**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5986
N/A	04-Sep-2024	4.6	Improper input validation in ThemeCenter prior to SMR Sep-2024 Release 1 allows physical attackers to install privileged applications. **CVE ID: CVE-2024-34645**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5987
Improper Limitation of a Pathname to a Restricted Directory	04-Sep-2024	4.6	Path Traversal in My Files prior to SMR Sep-2024 Release 1 allows physical attackers to access	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5988

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
('Path Traversal')			directories with My Files' privilege. **CVE ID: CVE-2024-34653**		
N/A	04-Sep-2024	3.3	Improper access control vulnerability in BGProtectManager prior to SMR Sep-2024 Release 1 allows local attackers to bypass restriction of process expiration. **CVE ID: CVE-2024-34640**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5989
N/A	04-Sep-2024	3.3	Improper Export of Android Application Components in FeliCaTest prior to SMR Sep-2024 Release 1 allows local attackers to enable NFC configuration. **CVE ID: CVE-2024-34641**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5990
Incorrect Authorization	04-Sep-2024	3.3	Incorrect authorization in kperfmon prior to SMR Sep-2024 Release 1 allows local attackers to access information related to performance including app usage. **CVE ID: CVE-2024-34652**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5991

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 13.0					
Improper Handling of Exceptional Conditions	04-Sep-2024	7.1	Improper handling of exceptional conditions in ThemeCenter prior to SMR Sep-2024 Release 1 allows local attackers to delete non-preloaded applications. **CVE ID: CVE-2024-34638**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5992
N/A	04-Sep-2024	5.5	Improper access control in WindowManagerService prior to SMR Sep-2024 Release 1 in Android 12, and SMR Jun-2024 Release 1 in Android 13 and Android 14 allows local attackers to bypass restrictions on starting services from the background. **CVE ID: CVE-2024-34637**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5993
N/A	04-Sep-2024	5.5	Improper access control in DualDarManagerProxy prior to SMR Sep-2024 Release 1 allows local attackers to cause local permanent denial of service. **CVE ID: CVE-2024-34646**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5994

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
N/A	04-Sep-2024	5.5	Incorrect use of privileged API in DualDarManagerProxy prior to SMR Sep-2024 Release 1 allows local attackers to access privileged APIs related to knox without proper license. **CVE ID: CVE-2024-34647**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5995
Incorrect Default Permissions	04-Sep-2024	5.5	Improper Handling of Insufficient Permissions in KnoxMiscPolicy prior to SMR Sep-2024 Release 1 allows local attackers to access sensitive data. **CVE ID: CVE-2024-34648**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5996
Incorrect Authorization	04-Sep-2024	5.5	Improper authorization in My Files prior to SMR Sep-2024 Release 1 allows local attackers to access restricted data in My Files. **CVE ID: CVE-2024-34651**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5997
N/A	04-Sep-2024	5.5	Improper Export of android application component in My Files prior to SMR Sep-2024 Release 1 allows local attackers to access	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5998

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
			files with My Files' privilege. **CVE ID: CVE-2024-34654**		
N/A	04-Sep-2024	5.5	Incorrect use of privileged API in UniversalCredentialManager prior to SMR Sep-2024 Release 1 allows local attackers to access privileged API related to UniversalCredentialManager. **CVE ID: CVE-2024-34655**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/5999
Improper Handling of Exceptional Conditions	04-Sep-2024	4.6	Improper handling of exceptional conditions in Setupwizard prior to SMR Aug-2024 Release 1 allows physical attackers to bypass proper validation. **CVE ID: CVE-2024-34639**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=08	O-SAM-ANDR-200924/6000
Incorrect Authorization	04-Sep-2024	4.6	Improper authorization in One UI Home prior to SMR Sep-2024 Release 1 allows physical attackers to temporarily access sensitive information. **CVE ID: CVE-2024-34642**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/6001
N/A	04-Sep-2024	4.6	Improper input validation in	https://security.samsungmobile	O-SAM-ANDR-200924/6002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ThemeCenter prior to SMR Sep-2024 Release 1 allows physical attackers to install privileged applications. **CVE ID: CVE-2024-34645**	.com/securityUpdate.smsb?year=2024&month=09	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Sep-2024	4.6	Path Traversal in My Files prior to SMR Sep-2024 Release 1 allows physical attackers to access directories with My Files' privilege. **CVE ID: CVE-2024-34653**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/6003
N/A	04-Sep-2024	3.3	Improper access control vulnerability in BGProtectManager prior to SMR Sep-2024 Release 1 allows local attackers to bypass restriction of process expiration. **CVE ID: CVE-2024-34640**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/6004
N/A	04-Sep-2024	3.3	Improper Export of Android Application Components in FeliCaTest prior to SMR Sep-2024 Release 1 allows local attackers to enable NFC configuration.	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/6005

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
			CVE ID: CVE-2024-34641		
Incorrect Authorization	04-Sep-2024	3.3	Incorrect authorization in kperfmon prior to SMR Sep-2024 Release 1 allows local attackers to access information related to performance including app usage. **CVE ID: CVE-2024-34652**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=09	O-SAM-ANDR-200924/6006
Product: exynos_1080_firmware					
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200924/6007
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280,	https://semiconductor.samsung.com/support/quality-support/product-security-	O-SAM-EXYN-200924/6008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos 1380, and Exynos 1330. In the function slsi_rx_range_done_ind(), there is no input validation check on rtt_id coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27387**	updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27387/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27364/	O-SAM-EXYN-200924/6009
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos	https://semiconductor.samsung.com/support/quality-support/product-security-	O-SAM-EXYN-200924/6010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27366**	updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27366/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input validation check on a length coming from userspace, which can lead to integer overflow	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27367/	O-SAM-EXYN-200924/6011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and a potential heap over-read. **CVE ID: CVE-2024-27367**		
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_received_frame_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27368**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200924/6012
Product: exynos_1280_firmware					
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200924/6013

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
			slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**		
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_rx_range_done_ind(), there is no input validation check on rtt_id coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27387**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27387/	O-SAM-EXYN-200924/6014
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-	O-SAM-EXYN-200924/6015

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
			slsi_rx_roamed_ind (), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**	updates/cve-2024-27364/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27366**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27366/	O-SAM-EXYN-200924/6016
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/,	O-SAM-EXYN-200924/6017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read. **CVE ID: CVE-2024-27367**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27367/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_received_frame_ind(), there is no input validation check on a length coming from userspace, which can lead to a	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200924/6018

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
			potential heap over-read. **CVE ID: CVE-2024-27368**		
Product: exynos_1330_firmware					
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200924/6019
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_rx_range_done_ind(), there is no input validation check on rtt_id coming from userspace, which can lead to a heap overwrite.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27387/	O-SAM-EXYN-200924/6020

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
			CVE ID: CVE-2024-27387		
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27364/	O-SAM-EXYN-200924/6021
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27366/	O-SAM-EXYN-200924/6022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27366**		
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read. **CVE ID: CVE-2024-27367**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27367/	O-SAM-EXYN-200924/6023
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200924/6024

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
			Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_received_frame_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27368**		
Product: exynos_1380_firmware					
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200924/6025

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
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_rx_range_done_ind(), there is no input validation check on rtt_id coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27387**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27387/	O-SAM-EXYN-200924/6026
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27364/	O-SAM-EXYN-200924/6027

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
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27366**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27366/	O-SAM-EXYN-200924/6028
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27367/	O-SAM-EXYN-200924/6029

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
			validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read. **CVE ID: CVE-2024-27367**		
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_received_frame_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27368**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200924/6030
Product: exynos_1480_firmware					
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos	https://semiconductor.samsung.com/support/quality-	O-SAM-EXYN-200924/6031

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
			980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**	support/product-security-updates/	
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_rx_range_done_ind(), there is no input validation check on rtt_id coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27387**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27387/	O-SAM-EXYN-200924/6032
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung	O-SAM-EXYN-200924/6033

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
			Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind (), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**	.com/support/quality-support/product-security-updates/cve-2024-27364/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27366**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27366/	O-SAM-EXYN-200924/6034

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
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read. **CVE ID: CVE-2024-27367**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27367/	O-SAM-EXYN-200924/6035
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_received_fra	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200924/6036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			me_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27368**		
Product: exynos_850_firmware					
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200924/6037
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_rx_range_done_ind(), there is no	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-	O-SAM-EXYN-200924/6038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input validation check on rtt_id coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27387**	support/product-security-updates/cve-2024-27387/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind (), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27364/	O-SAM-EXYN-200924/6039
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-	O-SAM-EXYN-200924/6040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27366**	support/product-security-updates/cve-2024-27366/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read. **CVE ID: CVE-2024-27367**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27367/	O-SAM-EXYN-200924/6041

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
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_received_frame_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27368**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200924/6042
Product: exynos_980_firmware					
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200924/6043

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
			from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**		
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_rx_range_done_ind(), there is no input validation check on rtt_id coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27387**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27387/	O-SAM-EXYN-200924/6044
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind(), there is no input validation check on a length coming from userspace,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27364/	O-SAM-EXYN-200924/6045

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
			which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**		
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27366**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27366/	O-SAM-EXYN-200924/6046
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/produc	O-SAM-EXYN-200924/6047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read. **CVE ID: CVE-2024-27367**	t-security-updates/cve-2024-27367/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_received_frame_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27368**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200924/6048
Product: exynos_w920_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 versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200924/6049
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_rx_range_done_ind(), there is no input validation check on rtt_id coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27387**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27387/	O-SAM-EXYN-200924/6050
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor,	https://semiconductor.samsung.com/support/q	O-SAM-EXYN-200924/6051

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
			Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind (), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**	uality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27364/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27366/	O-SAM-EXYN-200924/6052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential heap over-read. **CVE ID: CVE-2024-27366**		
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read. **CVE ID: CVE-2024-27367**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27367/	O-SAM-EXYN-200924/6053
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200924/6054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos W920, Exynos W930. In the function slsi_rx_received_frame_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27368**		
Product: exynos_w930_firmware					
Affected Version(s): -					
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_get_scan_extra_ies(), there is no input validation check on default_ies coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27383**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200924/6055
Out-of-bounds Write	09-Sep-2024	7.8	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and	https://semiconductor.samsung.com/support/quality-support/product-security-updates/,	O-SAM-EXYN-200924/6056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos 1330. In the function slsi_rx_range_done_ind(), there is no input validation check on rtt_id coming from userspace, which can lead to a heap overwrite. **CVE ID: CVE-2024-27387**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27387/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_roamed_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27364**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27364/	O-SAM-EXYN-200924/6057
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor Exynos Exynos 980, Exynos	https://semiconductor.samsung.com/support/quality-support/product-security-updates/,	O-SAM-EXYN-200924/6058

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
			850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_done_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27366**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27366/	
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_scan_ind(), there is no input validation check on a length coming from userspace, which can lead to integer overflow and a potential heap over-read.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/, https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2024-27367/	O-SAM-EXYN-200924/6059

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
			CVE ID: CVE-2024-27367		
Out-of-bounds Read	09-Sep-2024	5.5	An issue was discovered in Samsung Mobile Processor Exynos Mobile Processor, Wearable Processor Exynos 980, Exynos 850, Exynos 1080, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 1480, Exynos W920, Exynos W930. In the function slsi_rx_received_frame_ind(), there is no input validation check on a length coming from userspace, which can lead to a potential heap over-read. **CVE ID: CVE-2024-27368**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200924/6060
Vendor: totolink					
Product: t10_firmware					
Affected Version(s): 4.1.8cu.5207					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-2024	8.8	A vulnerability, which was classified as critical, was found in TOTOLINK AC1200 T8 and AC1200 T10 4.1.5cu.861_B20230220/4.1.8cu.5207. This affects the function	N/A	O-TOT-T10_-200924/6061

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
			setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument desc leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8573**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-2024	8.8	A vulnerability was found in TOTOLINK AC1200 T8 and AC1200 T10 4.1.5cu.861_B20230220/4.1.8cu.5207. It has been classified as critical. Affected is the function setIpPortFilterRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument desc leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the	N/A	O-TOT-T10_-200924/6062

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
			public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8576**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-2024	8.8	A vulnerability was found in TOTOLINK AC1200 T8 and AC1200 T10 4.1.5cu.861_B20230220/4.1.8cu.5207. It has been declared as critical. Affected by this vulnerability is the function setStaticDhcpRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument desc leads to buffer overflow. 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-2024-8577**	N/A	O-TOT-T10_-200924/6063
Product: t8_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 versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 4.1.5cu.861_b20230220					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-2024	9.8	A vulnerability classified as critical has been found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220. This affects the function setWiFiRepeaterCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument password leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8579**	N/A	O-TOT-T8_F-200924/6064
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-2024	8.8	A vulnerability, which was classified as critical, was found in TOTOLINK AC1200 T8 and AC1200 T10 4.1.5cu.861_B20230220/4.1.8cu.5207. This affects the function setParentalRules of the file /cgi-bin/cstecgi.cgi. The	N/A	O-TOT-T8_F-200924/6065

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
			manipulation of the argument desc leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8573**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Sep-2024	8.8	A vulnerability has been found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220 and classified as critical. This vulnerability affects the function setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument slaveIpList leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early	N/A	O-TOT-T8_F-200924/6066

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
			about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8574**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-2024	8.8	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220 and classified as critical. This issue affects the function setWiFiScheduleCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument desc leads to buffer overflow. 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-2024-8575**	N/A	O-TOT-T8_F-200924/6067
Buffer Copy without Checking Size of Input ('Classic	08-Sep-2024	8.8	A vulnerability was found in TOTOLINK AC1200 T8 and AC1200 T10 4.1.5cu.861_B20230220/4.1.8cu.5207. It has been classified as critical.	N/A	O-TOT-T8_F-200924/6068

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 Overflow')			Affected is the function setIpPortFilterRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument desc leads to buffer overflow. 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-2024-8576**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-2024	8.8	A vulnerability was found in TOTOLINK AC1200 T8 and AC1200 T10 4.1.5cu.861_B20230220/4.1.8cu.5207. It has been declared as critical. Affected by this vulnerability is the function setStaticDhcpRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument desc leads to buffer overflow. The attack can be launched remotely.	N/A	O-TOT-T8_F-200924/6069

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 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-2024-8577**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-2024	8.8	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220. It has been rated as critical. Affected by this issue is the function setWiFiMeshName of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument device_name leads to buffer overflow. 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-2024-8578**	N/A	O-TOT-T8_F-200924/6070

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
Use of Hard-coded Password	08-Sep-2024	8.1	A vulnerability classified as critical was found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220. This vulnerability affects unknown code of the file /etc/shadow.sample. The manipulation leads to use of hard-coded password. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8580**	N/A	O-TOT-T8_F-200924/6071
Vendor: wayos					
Product: fbm-291w_firmware					
Affected Version(s): 19.09.11					
Improper Neutralization of Special Elements	04-Sep-2024	6.8	WAYOS FBM-291W v19.09.11 is vulnerable to Command	N/A	O-WAY-FBM--200924/6072

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
used in a Command ('Command Injection')			Execution via msp_info_htm. **CVE ID: CVE-2024-44383**		
Vendor: yubico					
Product: security_key_c_nfc_by_yubico_firmware					
Affected Version(s): * Up to (excluding) 5.7					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**	https://www.yubico.com/support/security-advisories/ysa-2024-03/	O-YUB-SECU-200924/6073
Product: security_key_nfc_by_yubico_firmware					
Affected Version(s): * Up to (excluding) 5.7					

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
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**	https://www.yubico.com/support/security-advisories/ysa-2024-03/	O-YUB-SECU-200924/6074
Product: yubihsm_2_fips_firmware					
Affected Version(s): * Up to (excluding) 2.4.0					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires	https://www.yubico.com/support/security-advisories/ysa-2024-03/	O-YUB-YUBI-200924/6075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**		
Product: yubihsm_2_firmware					
Affected Version(s): * Up to (excluding) 2.4.0					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the	https://www.yubico.com/support/security-advisories/ysa-2024-03/	O-YUB-YUBI-200924/6076

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
			Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**		
Product: yubikey_5ci_fips_firmware					
Affected Version(s): * Up to (excluding) 5.7					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected.	https://www.yubico.com/support/security-advisories/ysa-2024-03/	O-YUB-YUBI-200924/6077

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
			CVE ID: CVE-2024-45678		
Product: yubikey_5ci_firmware					
Affected Version(s): * Up to (excluding) 5.7					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**	https://www.yubico.com/support/security-advisories/ysa-2024-03/	O-YUB-YUBI-200924/6078
Product: yubikey_5c_fips_firmware					
Affected Version(s): * Up to (excluding) 5.7					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with	https://www.yubico.com/support/security-	O-YUB-YUBI-200924/6079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**	advisories/ysa-2024-03/	
Product: yubikey_5c_firmware					
Affected Version(s): * Up to (excluding) 5.7					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic	https://www.yubico.com/support/security-advisories/ysa-2024-03/	O-YUB-YUBI-200924/6080

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
			side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**		
Product: yubikey_5c_nano_fips_firmware					
Affected Version(s): * Up to (excluding) 5.7					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an	https://www.yubico.com/support/security-advisories/ysa-2024-03/	O-YUB-YUBI-200924/6081

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
			Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**		
Product: yubikey_5c_nano_firmware					
Affected Version(s): * Up to (excluding) 5.7					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**	https://www.yubico.com/support/security-advisories/ysa-2024-03/	O-YUB-YUBI-200924/6082
Product: yubikey_5c_nfc_fips_firmware					
Affected Version(s): * Up to (excluding) 5.7					

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
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**	https://www.yubico.com/support/security-advisories/ysa-2024-03/	O-YUB-YUBI-200924/6083
Product: yubikey_5c_nfc_firmware					
Affected Version(s): * Up to (excluding) 5.7					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires	https://www.yubico.com/support/security-advisories/ysa-2024-03/	O-YUB-YUBI-200924/6084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**		
Product: yubikey_5_nano_fips_firmware					
Affected Version(s): * Up to (excluding) 5.7					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the	https://www.yubico.com/support/security-advisories/ysa-2024-03/	O-YUB-YUBI-200924/6085

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
			Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**		
Product: yubikey_5_nano_firmware					
Affected Version(s): * Up to (excluding) 5.7					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected.	https://www.yubico.com/support/security-advisories/ysa-2024-03/	O-YUB-YUBI-200924/6086

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
			CVE ID: CVE-2024-45678		
Product: yubikey_5_nfc_fips_firmware					
Affected Version(s): * Up to (excluding) 5.7					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**	https://www.yubico.com/support/security-advisories/ysa-2024-03/	O-YUB-YUBI-200924/6087
Product: yubikey_5_nfc_firmware					
Affected Version(s): * Up to (excluding) 5.7					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with	https://www.yubico.com/support/security-	O-YUB-YUBI-200924/6088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**	advisories/ysa-2024-03/	
Product: yubikey_bio_firmware					
Affected Version(s): * Up to (excluding) 5.7.2					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic	https://www.yubico.com/support/security-advisories/ysa-2024-03/	O-YUB-YUBI-200924/6089

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
			side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**		
Product: yubikey_c_bio_firmware					
Affected Version(s): * Up to (excluding) 5.7.2					
Observable Discrepancy	03-Sep-2024	4.2	Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an	https://www.yubico.com/support/security-advisories/ysa-2024-03/	O-YUB-YUBI-200924/6090

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
			Infineon cryptographic library may also be affected. **CVE ID: CVE-2024-45678**		
Vendor: Zyxel					
Product: ax7501-b0_firmware					
Affected Version(s): * Up to (excluding) 5.17\\(abpc.5.2\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-AX75-200924/6091
Product: ax7501-b1_firmware					
Affected Version(s): * Up to (excluding) 5.17\\(abpc.5.2\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-	O-ZYX-AX75-200924/6092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: dx3300-t0_firmware					
Affected Version(s): * Up to (excluding) 5.50\\(abvy.5.3\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-DX33-200924/6093
Product: dx3300-t1_firmware					
Affected Version(s): * Up to (excluding) 5.50\\(abvy.5.3\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-	O-ZYX-DX33-200924/6094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	extender-and-security-router-devices-09-03-2024	
Product: dx3301-t0_firmware					
Affected Version(s): * Up to (excluding) 5.50\\(abvy.5.3\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-DX33-200924/6095
Product: dx4510-b0_firmware					
Affected Version(s): * Up to (excluding) 5.17\\(abyl.7\\)b2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-	O-ZYX-DX45-200924/6096

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
			CVE ID: CVE-2024-5412	devices-09-03-2024	
Product: dx5401-b0_firmware					
Affected Version(s): * Up to (excluding) 5.17\\(abyo.6.2\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-DX54-200924/6097
Product: dx5401-b1_firmware					
Affected Version(s): * Up to (excluding) 5.17\\(abyo.6.2\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-DX54-200924/6098

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
Product: emg3525-t50b_firmware					
Affected Version(s): * Up to (excluding) 5.50\\(abpm.9.2\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-EMG3-200924/6099
Product: emg5523-t50b_firmware					
Affected Version(s): * Up to (excluding) 5.50\\(abpm.9.2\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-EMG5-200924/6100
Product: emg5723-t50k_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 5.50\\(abom.8.4\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-EMG5-200924/6101
Product: ex3300-t0_firmware					
Affected Version(s): * Up to (excluding) 5.50\\(abvy.5.3\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-EX33-200924/6102
Product: ex3300-t1_firmware					
Affected Version(s): * Up to (excluding) 5.50\\(abvy.5.3\\)c0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-EX33-200924/6103
Product: ex3301-t0_firmware					
Affected Version(s): * Up to (excluding) 5.50\\(abvy.5.3\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-EX33-200924/6104
Product: ex3500-t0_firmware					
Affected Version(s): * Up to (excluding) 5.44\\(achr.2\\)c0					
Buffer Copy	03-Sep-2024	7.5	A buffer overflow vulnerability in the	https://www.zyxel.com/global/	O-ZYX-EX35-200924/6105

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
without Checking Size of Input ('Classic Buffer Overflow')			library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: ex3501-t0_firmware					
Affected Version(s): * Up to (excluding) 5.44\\(achr.2\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-EX35-200924/6106
Product: ex3510-b0_firmware					
Affected Version(s): * Up to (excluding) 5.17\\(abup.12\\)b2					
Buffer Copy without Checking	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel	https://www.zyxel.com/global/en/support/security-	O-ZYX-EX35-200924/6107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: ex5401-b0_firmware					
Affected Version(s): * Up to (excluding) 5.17\\(abyo.6.2\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-EX54-200924/6108
Product: ex5401-b1_firmware					
Affected Version(s): * Up to (excluding) 5.17\\(abyo.6.2\\)c0					
Buffer Copy without Checking Size of Input	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-	O-ZYX-EX54-200924/6109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: ex5510-b0_firmware					
Affected Version(s): * Up to (excluding) 5.17\\(abqx.10\\)b2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-EX55-200924/6110
Product: ex5512-t0_firmware					
Affected Version(s): * Up to (excluding) 5.70\\(aceg.3\\)c2					
Buffer Copy without Checking Size of Input ('Classic	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-	O-ZYX-EX55-200924/6111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: ex5601-t0_firmware					
Affected Version(s): * Up to (excluding) 5.70\\(acdz.3.2\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-EX56-200924/6112
Product: ex5601-t1_firmware					
Affected Version(s): * Up to (excluding) 5.70\\(acdz.3.2\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-	O-ZYX-EX56-200924/6113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: ex7501-b0_firmware					
Affected Version(s): * Up to (excluding) 5.18\\(achn.1.2\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-EX75-200924/6114
Product: ex7710-b0_firmware					
Affected Version(s): * Up to (excluding) 5.18\\(acak.1\\)c1					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-	O-ZYX-EX77-200924/6115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: nebula_fwa505_firmware					
Affected Version(s): * Up to (excluding) 1.18\\(acko.4\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-NEBU-200924/6116
Product: nebula_fwa510_firmware					
Affected Version(s): * Up to (excluding) 1.18\\(acgd.4\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-	O-ZYX-NEBU-200924/6117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	extender-and-security-router-devices-09-03-2024	
Product: nebula_fwa710_firmware					
Affected Version(s): * Up to (excluding) 1.18\\(acgc.4\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-NEBU-200924/6118
Product: nebula_lte3301-plus_firmware					
Affected Version(s): * Up to (excluding) 1.18\\(acca.4\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-	O-ZYX-NEBU-200924/6119

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
			CVE ID: CVE-2024-5412	devices-09-03-2024	
Product: nr5103ev2_firmware					
Affected Version(s): * Up to (excluding) 1.00\\(aciq.1\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-NR51-200924/6120
Product: nr5103_firmware					
Affected Version(s): * Up to (excluding) 4.19\\(abyc.6\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-NR51-200924/6121

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
Product: nr5307_firmware					
Affected Version(s): * Up to (excluding) 1.00\\(acjt.0\\)b6					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-NR53-200924/6122
Product: nr7103_firmware					
Affected Version(s): * Up to (excluding) 1.00\\(accz.4\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-NR71-200924/6123
Product: nr7302_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 versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.00\\(acha.4\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-NR73-200924/6124
Product: nr7303_firmware					
Affected Version(s): * Up to (excluding) 1.00\\(acei.1\\)b4					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-NR73-200924/6125
Product: nr7501_firmware					
Affected Version(s): * Up to (excluding) 1.00\\(aceh.1\\)c0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-NR75-200924/6126
Product: nwa110ax_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(abtg.2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1)	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-NWA1-200924/6127

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
			and earlier, and USG LITE 60AX firmware version V2.00(ACIP .2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: nwa1123-ac_pro_firmware					
Affected Version(s): * Up to (excluding) 6.28\\(abhd.3\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP .2) could allow an	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-NWA1-200924/6128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: nwa1123acv3_firmware					
Affected Version(s): * Up to (excluding) 6.70\\(abvt.5\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-NWA1-200924/6129

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
			cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: nwa130be_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(acil.2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-NWA1-200924/6130

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
Product: nwa210ax_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(abtd.2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-NWA2-200924/6131
Product: nwa220ax-6e_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(acco.2\\)					
Improper Neutralization of	03-Sep-2024	9.8	The improper neutralization of special elements in	https://www.zyxel.com/global/en/support/sec	O-ZYX-NWA2-200924/6132

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
Special Elements used in an OS Command ('OS Command Injection')			the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	urity-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	
Product: nwa50ax_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(abyw.2\\)					
Improper Neutralization of Special Elements used in an OS Command	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-	O-ZYX-NWA5-200924/6133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	
Product: nwa50ax_pro_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(acge.2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4)	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-	O-ZYX-NWA5-200924/6134

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
			and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	devices-09-03-2024	
Product: nwa55axe_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(abzl.2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-NWA5-200924/6135

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
			firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: nwa90ax_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(accv.2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-NWA9-200924/6136

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
			firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: nwa90ax_pro_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(acgf.2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-NWA9-200924/6137

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
			OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: pm3100-t0_firmware					
Affected Version(s): * Up to (excluding) 5.42\\(acbf.2.1\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-PM31-200924/6138
Product: pm5100-t0_firmware					
Affected Version(s): * Up to (excluding) 5.42\\(acbf.2.1\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-	O-ZYX-PM51-200924/6139

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
			HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	extender-and-security-router-devices-09-03-2024	
Product: pm7300-t0_firmware					
Affected Version(s): * Up to (excluding) 5.42\\(abyy.2.2\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-PM73-200924/6140
Product: px3321-t1_firmware					
Affected Version(s): * Up to (excluding) 5.44\\(acjb.0.2\\)z0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-	O-ZYX-PX33-200924/6141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-5412	devices-09-03-2024	
Product: scr50axe_firmware					
Affected Version(s): * Up to (excluding) 1.10\\(acgn.3\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-SCR5-200924/6142
Product: usg_lite_60ax_firmware					
Affected Version(s): * Up to (excluding) v2.00\\(acip.3\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-USG_-200924/6143

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
			earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP .2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: vmg3625-t50b_firmware					
Affected Version(s): * Up to (excluding) 5.50\\(abpm.9.2\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-VMG3-200924/6144
Product: vmg3927-t50k_firmware					
Affected Version(s): * Up to (excluding) 5.50\\(abom.8.4\\)c0					
Buffer Copy	03-Sep-2024	7.5	A buffer overflow vulnerability in the	https://www.zyxel.com/global/	O-ZYX-VMG3-200924/6145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: vmg4005-b50a_firmware					
Affected Version(s): * Up to (excluding) 5.15\\(abqa.2.2\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-VMG4-200924/6146
Product: vmg4005-b60a_firmware					
Affected Version(s): * Up to (excluding) 5.15\\(abqa.2.2\\)c0					
Buffer Copy without Checking	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel	https://www.zyxel.com/global/en/support/security-	O-ZYX-VMG4-200924/6147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: vmg8623-t50b_firmware					
Affected Version(s): * Up to (excluding) 5.50\\(abpm.9.2\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-VMG8-200924/6148
Product: vmg8825-t50k_firmware					
Affected Version(s): * Up to (excluding) 5.50\\(abom.8.4\\)c0					
Buffer Copy without Checking Size of Input	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-	O-ZYX-VMG8-200924/6149

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
('Classic Buffer Overflow')			5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: wac500h_firmware					
Affected Version(s): * Up to (excluding) 6.70\\(abwa.5\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-WAC5-200924/6150

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
			OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: wac500_firmware					
Affected Version(s): * Up to (excluding) 6.70\\(abvs.5\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-WAC5-200924/6151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7261		
Product: wac6103d-i_firmware					
Affected Version(s): * Up to (excluding) 6.28\\(aaxh.3\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-WAC6-200924/6152
Product: wac6502d-s_firmware					
Affected Version(s): * Up to (excluding) 6.28\\(aase.3\\)					

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 Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-WAC6-200924/6153
Product: wac6503d-s_firmware					
Affected Version(s): * Up to (excluding) 6.28\\(aasf.3\\)					
Improper Neutralization of Special Elements	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI	https://www.zyxel.com/global/en/support/security-advisories/zyxe	O-ZYX-WAC6-200924/6154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	l-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	
Product: wac6552d-s_firmware					
Affected Version(s): * Up to (excluding) 6.28\\(abio.3\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-	O-ZYX-WAC6-200924/6155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP .2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	aps-and-security-router-devices-09-03-2024	
Product: wac6553d-e_firmware					
Affected Version(s): * Up to (excluding) 6.28\\(aasg.3\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-WAC6-200924/6156

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
			firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: wax300h_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(achf.2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1)	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-WAX3-200924/6157

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
			and earlier, and USG LITE 60AX firmware version V2.00(ACIP .2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: wax510d_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(abtf.2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-WAX5-200924/6158

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
			.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: wax610d_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(abte.2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-WAX6-200924/6159

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
			cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: wax620d-6e_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(accn.2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-WAX6-200924/6160

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
Product: wax630s_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(abzd.2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-WAX6-200924/6161
Product: wax640s-6e_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(accm.2\\)					
Improper Neutralization of	03-Sep-2024	9.8	The improper neutralization of special elements in	https://www.zyxel.com/global/en/support/sec	O-ZYX-WAX6-200924/6162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	urity-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	
Product: wax650s_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(abrm.2\\)					
Improper Neutralization of Special Elements used in an OS Command	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-	O-ZYX-WAX6-200924/6163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	
Product: wax655e_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(acdo.2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4)	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-	O-ZYX-WAX6-200924/6164

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
			and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**	devices-09-03-2024	
Product: wbe530_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(acle.2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-WBE5-200924/6165

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
			firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: wbe660s_firmware					
Affected Version(s): * Up to (excluding) 7.00\\(acgg.2\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	9.8	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024	O-ZYX-WBE6-200924/6166

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
			firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device. **CVE ID: CVE-2024-7261**		
Product: wx3100-t0_firmware					
Affected Version(s): * Up to (excluding) 5.50\\(abvl.4.2\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-WX31-200924/6167
Product: wx3401-b0_firmware					
Affected Version(s): * Up to (excluding) 5.17\\(abve.2.5\\)c0					
Buffer Copy without Checking Size of Input ('Classic	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-	O-ZYX-WX34-200924/6168

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 Overflow')			attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	
Product: wx5600-t0_firmware					
Affected Version(s): * Up to (excluding) 5.70\\(aceb.3.2\\)c0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	7.5	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-5412**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-some-5g-nr-cpe-dsl-ethernet-cpe-fiber-ont-wifi-extender-and-security-router-devices-09-03-2024	O-ZYX-WX56-200924/6169
Product: zld_firmware					
Affected Version(s): From (including) 4.16 Up to (excluding) 5.39					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	8.1	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	O-ZYX-ZLD_-200924/6170

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
			V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username exceeding 28 characters exists. **CVE ID: CVE-2024-42057**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	O-ZYX-ZLD_-200924/6171

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
			V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device. **CVE ID: CVE-2024-42060**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	O-ZYX-ZLD_-200924/6172

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
			series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. The attacker could obtain browser-based information if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	O-ZYX-ZLD_-200924/6173

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
			sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-6343**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.39					
NULL Pointer Dereference	03-Sep-2024	7.5	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	O-ZYX-ZLD_-200924/6174
Affected Version(s): From (including) 4.32 Up to (excluding) 5.39					
Improper Neutralization of Special Elements used in an OS	03-Sep-2024	8.1	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-	O-ZYX-ZLD_-200924/6175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username exceeding 28 characters exists. **CVE ID: CVE-2024-42057**	multiple-vulnerabilities-in-firewalls-09-03-2024	
NULL Pointer Dereference	03-Sep-2024	7.5	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-	O-ZYX-ZLD_-200924/6176

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
			series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**	multiple-vulnerabilities-in-firewalls-09-03-2024	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	O-ZYX-ZLD_-200924/6177

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
			attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device. **CVE ID: CVE-2024-42060**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. The attacker could obtain browser-based information	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	O-ZYX-ZLD_-200924/6178

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
			if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-6343**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	O-ZYX-ZLD_-200924/6179
Affected Version(s): From (including) 4.50 Up to (excluding) 5.39					
Improper Neutralization of Special	03-Sep-2024	8.1	A command injection vulnerability in the IPSec VPN feature	https://www.zyxel.com/global/en/support/security-	O-ZYX-ZLD_-200924/6180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username exceeding 28 characters exists. **CVE ID: CVE-2024-42057**	advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	
NULL Pointer Dereference	03-Sep-2024	7.5	A null pointer dereference vulnerability in Zyxel ATP series	https://www.zyxel.com/global/en/support/security-	O-ZYX-ZLD_-200924/6181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device. **CVE ID: CVE-2024-42058**	advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	O-ZYX-ZLD_-200924/6182

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
			V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device. **CVE ID: CVE-2024-42060**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-2024	6.1	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	O-ZYX-ZLD_-200924/6183

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 attacker could obtain browser-based information if the malicious script is executed on the victim's browser. **CVE ID: CVE-2024-42061**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Sep-2024	4.9	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device. **CVE ID: CVE-2024-6343**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	O-ZYX-ZLD_-200924/6184
Affected Version(s): From (including) 4.60 Up to (excluding) 5.39					

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 Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.60 through V5.38 and USG FLEX series firmware versions from V4.60 through V5.38 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device by executing a crafted CLI command. **CVE ID: CVE-2024-7203**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	O-ZYX-ZLD_-200924/6185
Affected Version(s): From (including) 5.00 Up to (excluding) 5.39					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Sep-2024	7.2	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through V5.38, USG FLEX series firmware versions from V5.00 through V5.38, USG FLEX 50(W) series firmware versions from V5.00 through V5.38, and USG20(W)-VPN	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024	O-ZYX-ZLD_-200924/6186

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
			series firmware versions from V5.00 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted compressed language file via FTP. **CVE ID: CVE-2024-42059**		

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